(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号
特開2002－374261
（P2002－374261A）
(43)公開日　平成14年12月26日(2002.12.26)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード*(参考)
Ｈ０４Ｌ　12/28	３００	Ｈ０４Ｌ　12/28	３００Ｚ	５Ｋ０３３
Ｇ０６Ｆ　1/00	３７０	Ｇ０６Ｆ　1/00	３７０Ｅ	５Ｋ０６７
Ｈ０４Ｑ　7/38		Ｈ０４Ｂ　7/26	１０９Ｒ	

審査請求　未請求　請求項の数30　ＯＬ　（全 28 頁）

(21)出願番号　特願2001－183315(P2001－183315)

(22)出願日　平成13年６月18日(2001.6.18)

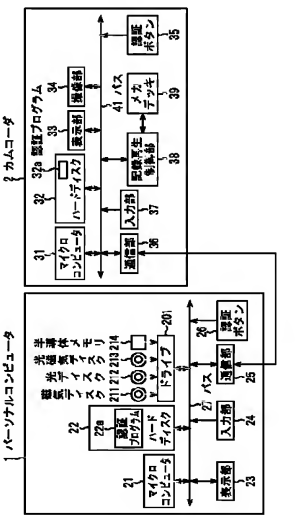
(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号
(72)発明者　松野　克巳
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(74)代理人　100082131
弁理士　稲本　義雄

Ｆターム(参考)　5K033 BA01 CC01 DA17
5K067 AA34 BB04 BB21 DD17 DD30
EE02 EE12 HH22

(54)【発明の名称】　情報処理装置および方法、情報処理システム、記録媒体、並びにプログラム

(57)【要約】
【課題】　ブルートゥースによる電子機器間の相互認証を容易に実現させる。
【解決手段】　ユーザは、パーソナルコンピュータ１とカムコーダ２の相互認証をさせるとき、双方の認証ボタン２６，３５を同時に押下する。その結果、パーソナルコンピュータ１の認証プログラム２２ａと、カムコーダ２の認証プログラム３２ａは、相互の認証ボタン２６，３５がオンにされた時刻とオフにされた時刻を検出し、相互にその時刻の情報を交換して、所定の時間差の範囲内で一致すると判定するとき、相互に認証処理がなされているものとみなし、認証を認める。

図4



【特許請求の範囲】
【請求項１】　ネットワークを介して他の情報処理装置と接続される情報処理装置において、
オンオフを入力する入力手段と、
前記入力手段によりオンが入力された第１のタイミングを計測する第1のタイ
ミング計測手段と、前記入力手段によりオフが入力された第２のタイミングを計測する第２のタイミング計測手段と、
前記第１のタイミング、および、前記第２のタイミングを前記ネットワークを介して他の情報処理装置に送信する送信手段とを備えることを特徴とする情報処理装置。
【請求項２】　前記ネットワークは、ブルートゥースにより構成されることを特徴とする請求項１に記載の情報処理装置。
【請求項３】　前記第１のタイミング計測手段、および、前記第２のタイミング計測手段は、いずれも複数回数のタイミングを計測することを特徴とする請求項１に記載の情報処理装置。
【請求項４】　ネットワークを介して他の情報処理装置と接続される情報処理装置の情報処理方法において、
オンオフを入力する入力手段と、
前記入力ステップの処理でオンが入力された第１のタイミングを計測する第1のタイミング計測ステップと、
前記入力ステップの処理でオフが入力された第２のタイミングを計測する第２のタイミング計測ステップと、
前記第１のタイミング、および、前記第２のタイミングを前記ネットワークを介して他の情報処理装置に送信する送信ステップとを含むことを特徴とする情報処理方法。
【請求項５】　ネットワークを介して他の情報処理装置と接続される情報処理装置を制御するプログラムであって、
オンオフの入力を制御する入力制御手段と、
前記入力制御ステップの処理でオンが入力された第１のタイミングの計測を制御する第1のタイミング計測制御ステップと、
前記入力制御ステップの処理でオフが入力された第２のタイミングの計測を制御する第２のタイミング計測制御ステップと、
前記第１のタイミング、および、前記第２のタイミングの前記ネットワークを介した他の情報処理装置への送信を制御する送信制御ステップとを含むことを特徴とするコンピュータが読み取り可能なプログラムが記録されている記録媒体。
【請求項６】　ネットワークを介して他の情報処理装置と接続される情報処理装置を制御するコンピュータに、
オンオフの入力を制御する入力制御手段と、
前記入力制御ステップの処理でオンが入力された第１のタイミングの計測を制御する第1のタイミング計測制御ステップと、
前記入力制御ステップの処理でオフが入力された第２のタイミングの計測を制御する第２のタイミング計測制御ステップと、
前記第１のタイミング、および、前記第２のタイミングの前記ネットワークを介した他の情報処理装置への送信を制御する送信制御ステップとを実行させるプログラム。
【請求項７】　ネットワークを介して他の情報処理装置と接続される情報処理装置において、
オンオフを入力する入力手段と、
前記入力手段によりオンが入力された第１のタイミングを計測する第1のタイミング計測手段と、
前記入力手段によりオフが入力された第２のタイミングを計測する第２のタイミング計測手段と、
前記他の情報処理装置より送信されてくる、前記他の情報処理装置の他の入力手段によりオンが入力された第３のタイミング、および、オフが入力された第４のタイミングを受信する受信手段と、
前記第１のタイミングと前記第３のタイミング、および、前記第２のタイミングと前記第４のタイミングを、それぞれ比較する比較手段と、
前記比較手段の比較結果に基づいて、前記他の情報処理装置との認証処理を実行する認証手段とを備えることを特徴とする情報処理装置。
【請求項８】　前記ネットワークは、ブルートゥースにより構成されることを特徴とする請求項７に記載の情報処理装置。
【請求項９】　前記比較手段は、前記第１のタイミングと前記第３のタイミング、および、前記第２のタイミングと第４のタイミングとの、それぞれの差を求めて、前記差が所定範囲内であるか否かを比較することを特徴とする請求項７に記載の情報処理装置。
【請求項１０】　前記認証手段は、前記それぞれの差が、いずれも前記所定の範囲内であるとき、前記他の情報処理装置を認証することを特徴とする請求項９に記載の情報処理装置。
【請求項１１】　前記第１のタイミング計測手段、および、前記第２のタイミング計測手段は、いずれも複数回数のタイミングを計測し、前記受信手段は、前記他の入力手段により複数回数オンが入力された第３のタイミング、および、複数回数オフにされた第４のタイミングを受信することを特徴とする請求項７に記載の情報処理装置。
【請求項１２】　ネットワークを介して他の情報処理装置と接続される情報処理装置の情報処理方法において、
オンオフを入力する入力ステップと、
前記入力ステップの処理でオンが入力された第１のタイミングを計測する第1のタイミング計測ステップと、
前記入力ステップの処理でオフが入力された第２のタイ

ミングを計測する第２のタイミング計測ステップと、
前記他の情報処理装置より送信されてくる、前記他の情報処理装置の他の入力ステップの処理でオンが入力された第３のタイミング、および、オフが入力された第４のタイミングを受信する受信手段と、
前記第１のタイミングと前記第３のタイミング、および、前記第２のタイミングと前記第４のタイミングを、それぞれ比較する比較ステップと、
前記比較ステップの処理での比較結果に基づいて、前記他の情報処理装置との認証処理を実行する認証ステップとを含むことを特徴とする情報処理方法。
【請求項１３】　ネットワークを介して他の情報処理装置と接続される情報処理装置を制御するプログラムであって、
オンオフの入力を制御する入力ステップと、
前記入力制御ステップの処理でオンが入力された第１のタイミングの計測を制御する第1のタイミング計測制御ステップと、
前記入力制御ステップの処理でオフが入力された第２のタイミングの計測を制御する第２のタイミング計測制御ステップと、
前記他の情報処理装置より送信されてくる、前記他の情報処理装置の他の入力制御ステップの処理でオンが入力された第３のタイミング、および、オフが入力された第４のタイミングの受信を制御する受信制御手段と、
前記第１のタイミングと前記第３のタイミング、および、前記第２のタイミングと前記第４のタイミングの、それぞれの比較を制御する比較制御ステップと、前記比較制御ステップの処理での比較結果に基づいて、前記他の情報処理装置との認証処理の実行を制御する認証制御ステップとを実行させるプログラムが記録されている記録媒体。
【請求項１４】　ネットワークを介して他の情報処理装置と接続される情報処理装置を制御するコンピュータに、
オンオフの入力を制御する入力ステップと、
前記入力制御ステップの処理でオンが入力された第１のタイミングの計測を制御する第1のタイミング計測制御ステップと、
前記入力制御ステップの処理でオフが入力された第２のタイミングの計測を制御する第２のタイミング計測制御ステップと、
前記他の情報処理装置より送信されてくる、前記他の情報処理装置の他の入力制御ステップの処理でオンが入力された第３のタイミング、および、オフが入力された第４のタイミングの受信を制御する受信制御手段と、
前記第１のタイミングと前記第３のタイミング、および、前記第２のタイミングと前記第４のタイミングの、それぞれの比較を制御する比較制御ステップと、前記比較制御ステップの処理での比較結果に基づいて、前記他の情報処理装置との認証処理の実行を制御する認証制御ステップとを実行させるプログラム。
【請求項１５】　ネットワークを介して相互に接続される第1の情報処理装置と第２の情報処理装置からなる情報処理システムにおいて、
第1の情報処理装置は、
オンオフを入力する第１の入力手段と、
前記第１の入力手段によりオンが入力された第１のタイミングを計測する第1のタイミング計測手段と、
前記第１の入力手段によりオフが入力された第２のタイミングを計測する第２のタイミング計測手段と、
前記第１のタイミング、および、前記第２のタイミングを前記ネットワークを介して前記第２の情報処理装置に送信する送信手段とを備え、
第２の情報処理装置は、オンオフを入力する第２の入力手段と、
前記第２の入力手段によりオンが入力されたタイミングを計測する第３のタイミング計測手段と、
前記第２の入力手段によりオフが入力されたタイミングを計測する第４のタイミング計測手段と、
前記第１の情報処理装置より送信されてくる、前記第１のタイミング、および、前記第２のタイミングを受信する受信手段と、
前記第１のタイミングと前記第３のタイミング、および、前記第２のタイミングと前記第４のタイミングとをそれぞれ比較する比較手段と、
前記比較手段の比較結果に基づいて、前記第１の情報処理装置との認証処理を実行する認証手段とを備えることを特徴とする情報処理システム。
【請求項１６】　ネットワークを介して相互に接続される第1の情報処理装置と第２の情報処理装置からなる情報処理システムの情報処理方法において、
第1の情報処理装置の情報処理方法は、
オンオフを入力する第１の入力ステップと、
前記第１の入力ステップの処理でオンが入力された第１のタイミングを計測する第1のタイミング計測ステップと、
前記第１の入力ステップの処理でオフが入力された第２のタイミングを計測する第２のタイミング計測ステップと、
前記第１のタイミング、および、前記第２のタイミングを前記ネットワークを介して前記第２の情報処理装置に送信する送信ステップとを含み、
第２の情報処理装置の情報処理方法は、
オンオフを入力する第２の入力ステップと、
前記第２の入力ステップの処理でオンが入力されたタイミングを計測する第３のタイミング計測ステップと、
前記第２の入力ステップの処理でオフが入力されたタイミングを計測する第４のタイミング計測ステップと、
前記第１の情報処理装置より送信されてくる、前記第１

のタイミング、および、前記第２のタイミングを受信する受信ステップと、
前記第１のタイミングと前記第３のタイミング、および、前記第２のタイミングと前記第４のタイミングとをそれぞれ比較する比較ステップと、
前記比較ステップの処理での比較結果に基づいて、前記第１の情報処理装置との認証処理を実行する認証ステップとを含むことを特徴とする情報処理システムの情報処理方法。

【請求項１７】　ネットワークを介して相互に接続される第1の情報処理装置と第２の情報処理装置からなる情報処理システムを制御するプログラムであって、
第1の情報処理装置を制御するプログラムは、
オンオフの入力を制御する第１の入力制御ステップと、
前記第１の入力制御ステップの処理でオンが入力された第１のタイミングの計測を制御する第1のタイミング計測制御ステップと、
前記第１の入力制御ステップの処理でオフが入力された第２のタイミングの計測を制御する第２のタイミング計測制御ステップと、
前記第１のタイミング、および、前記第２のタイミングの前記ネットワークを介した前記第２の情報処理装置への送信を制御する送信制御ステップとを含み、
第２の情報処理装置を制御するプログラムは、
オンオフの入力を制御する第２の入力制御ステップと、
前記第２の入力制御ステップの処理でオンが入力されたタイミングの計測を制御する第３のタイミング計測制御ステップと、
前記第２の入力制御ステップの処理でオフが入力されたタイミングの計測を制御する第４のタイミング計測制御ステップと、
前記第１の情報処理装置より送信されてくる、前記第１のタイミング、および、前記第２のタイミングの受信を制御する受信制御ステップと、
前記第１のタイミングと前記第３のタイミング、および、前記第２のタイミングと前記第４のタイミングとのそれぞれの比較を制御する比較制御ステップと、
前記比較制御ステップの処理での比較結果に基づいて、前記第１の情報処理装置との認証処理の実行を制御する認証制御ステップとを含むことを特徴とするコンピュータが読み取り可能なプログラムが記録されている記録媒体。

【請求項１８】　ネットワークを介して相互に接続される第1の情報処理装置と第２の情報処理装置からなる情報処理システムを制御するコンピュータのうち、
第1の情報処理装置を制御するコンピュータに、
オンオフの入力を制御する第１の入力制御ステップと、
前記第１の入力制御ステップの処理でオンが入力された第１のタイミングの計測を制御する第1のタイミング計測制御ステップと、
前記第１の入力制御ステップの処理でオフが入力された第２のタイミングの計測を制御する第２のタイミング計測制御ステップと、
前記第１のタイミング、および、前記第２のタイミングの前記ネットワークを介した前記第２の情報処理装置への送信を制御する送信制御ステップとを実行させ、
第２の情報処理装置を制御するコンピュータに、
オンオフの入力を制御する第２の入力制御ステップと、
前記第２の入力制御ステップの処理でオンが入力されたタイミングの計測を制御する第３のタイミング計測制御ステップと、
前記第２の入力制御ステップの処理でオフが入力されたタイミングの計測を制御する第４のタイミング計測制御ステップと、
前記第１の情報処理装置より送信されてくる、前記第１のタイミング、および、前記第２のタイミングの受信を制御する受信制御ステップと、
前記第１のタイミングと前記第３のタイミング、および、前記第２のタイミングと前記第４のタイミングとのそれぞれの比較を制御する比較制御ステップと、
前記比較制御ステップの処理での比較結果に基づいて、前記第１の情報処理装置との認証処理の実行を制御する認証制御ステップとを実行させるプログラム。

【請求項１９】　ネットワークを介して他の情報処理装置と接続される情報処理装置において、
オンオフを入力する入力手段と、
前記入力手段によりオンが入力された第１のタイミングを計測する第1のタイミング計測手段と、
前記入力手段によりオフが入力された第２のタイミングを計測する第２のタイミング計測手段と、
前記第１のタイミング、または、前記第２のタイミングを前記ネットワークを介して前記他の情報処理装置に送信する送信手段と、
前記他の情報処理装置より送信されてくる、前記送信手段により送信された前記第１のタイミング、または、前記第２のタイミングのいずれかに対応した、前記他の情報処理装置の他の入力手段によりオンが入力された第３のタイミング、または、オフが入力された第４のタイミングを受信する受信手段と、
前記第１のタイミングと前記第３のタイミング、または、前記第２のタイミングと前記第４のタイミングとを比較する比較手段と、
前記比較手段の比較結果に基づいて、前記他の情報処理装置との認証処理を実行する認証手段とを備えることを特徴とする情報処理装置。

【請求項２０】　前記ネットワークは、ブルートゥースにより構成されることを特徴とする請求項１９に記載の情報処理装置。

【請求項２１】　前記第１のタイミング計測手段、および、前記第２のタイミング計測手段は、いずれも複数回

数のタイミングを計測し、前記受信手段は、前記他の入力手段により複数回数オンが入力された第３のタイミング、および、複数回数オフにされた第４のタイミングを受信することを特徴とする請求項１９に記載の情報処理装置。

【請求項２２】　前記比較手段は、前記第１のタイミングと前記第３のタイミング、または、前記第２のタイミングと前記第４のタイミングとの差を求めて、前記差が所定範囲内になるか否かを比較することを特徴とする請求項１９に記載の情報処理装置。

【請求項２３】　前記認証手段は、前記差が、前記所定の範囲内であるとき、前記他の情報処理装置を認証することを特徴とする請求項２２に記載の情報処理装置。

【請求項２４】　ネットワークを介して他の情報処理装置と接続される情報処理装置の情報処理方法において、

オンオフを入力する入力ステップと、

前記入力ステップの処理でオンが入力された第１のタイミングを計測する第1のタイミング計測ステップと、

前記入力ステップの処理でオフが入力された第２のタイミングを計測する第２のタイミング計測ステップと、

前記第１のタイミング、または、前記第２のタイミングを前記ネットワークを介して前記他の情報処理装置に送信する送信ステップと、

前記他の情報処理装置より送信されてくる、前記送信ステップの処理で送信された前記第１のタイミング、または、前記第２のタイミングのいずれかに対応した、前記他の情報処理装置の他の入力ステップの処理でオンが入力された第３のタイミング、または、オフが入力された第４のタイミングを受信する受信ステップと、

前記第１のタイミングと前記第３のタイミング、または、前記第２のタイミングと前記第４のタイミングとを比較する比較ステップと、

前記比較ステップの処理での比較結果に基づいて、前記他の情報処理装置との認証処理を実行する認証ステップとを含むことを特徴とする情報処理方法。

【請求項２５】　ネットワークを介して他の情報処理装置と接続される情報処理装置を制御するプログラムであって、

オンオフの入力を制御する入力制御ステップと、

前記入力制御ステップの処理でオンが入力された第１のタイミングの計測を制御する第1のタイミング計測制御ステップと、

前記入力制御ステップの処理でオフが入力された第２のタイミングの計測を制御する第２のタイミング計測制御ステップと、

前記第１のタイミング、または、前記第２のタイミングの前記ネットワークを介した前記他の情報処理装置への送信を制御する送信制御ステップと、

前記他の情報処理装置より送信されてくる、前記送信制御ステップの処理で送信された前記第１のタイミング、または、前記第２のタイミングのいずれかに対応した、前記他の情報処理装置の他の入力制御ステップの処理でオンが入力された第３のタイミング、または、オフが入力された第４のタイミングの受信を制御する受信制御ステップと、

前記第１のタイミングと前記第３のタイミング、または、前記第２のタイミングと前記第４のタイミングとの比較を制御する比較制御ステップと、

前記比較制御ステップの処理での比較結果に基づいて、前記他の情報処理装置との認証処理の実行を制御する認証制御ステップとを含むことを特徴とするコンピュータが読み取り可能なプログラムが記録されている記録媒体。

【請求項２６】　ネットワークを介して他の情報処理装置と接続される情報処理装置を制御するコンピュータに、

オンオフの入力を制御する入力制御ステップと、

前記入力制御ステップの処理でオンが入力された第１のタイミングの計測を制御する第1のタイミング計測制御ステップと、

前記入力制御ステップの処理でオフが入力された第２のタイミングの計測を制御する第２のタイミング計測制御ステップと、

前記第１のタイミング、または、前記第２のタイミングの前記ネットワークを介した前記他の情報処理装置への送信を制御する送信制御ステップと、

前記他の情報処理装置より送信されてくる、前記送信制御ステップの処理で送信された前記第１のタイミング、または、前記第２のタイミングのいずれかに対応した、前記他の情報処理装置の他の入力制御ステップの処理でオンが入力された第３のタイミング、または、オフが入力された第４のタイミングの受信を制御する受信制御ステップと、

前記第１のタイミングと前記第３のタイミング、または、前記第２のタイミングと前記第４のタイミングとの比較を制御する比較制御ステップと、

前記比較制御ステップの処理での比較結果に基づいて、前記他の情報処理装置との認証処理の実行を制御する認証制御ステップとを実行させるプログラム。

【請求項２７】　ネットワークを介して相互に接続される、オンオフを入力する第１の入力手段と、前記第１の入力手段によりオンが入力された第１のタイミングを計測する第1のタイミング計測手段と、前記第１の入力手段によりオフが入力された第２のタイミングを計測する第２のタイミング計測手段と、前記第２のタイミングを前記ネットワークを介して第２の情報処理装置に送信する第１の送信手段とを備えた第１の情報処理装置と、オンオフを入力する第２の入力手段と、前記第２の入力手段によりオンが入力された第３のタイミングを計測する第３のタイミング計測手段と前記第２の入力手段により

オフが入力された第４のタイミングを計測する第４のタイミング計測手段と、前記第３のタイミングを前記ネットワークを介して第１の情報処理装置に送信する第２の送信手段とを備えた前記第２の情報処理装置から構成された情報処理システムにおいて、
前記第１の情報処理装置は、
前記第２の情報処理装置より送信されてくる、前記第３のタイミングを受信する第１の受信手段と、
前記第１のタイミングと前記第３のタイミングを比較する第１の比較手段と、
前記第１の比較手段の比較結果に基づいて、前記第２の情報処理装置との認証処理を実行する第１の認証手段とを備え、
前記第２の情報処理装置は、
前記第１の情報処理装置より送信されてくる、前記第２のタイミングを受信する第２の受信手段と、
前記第２のタイミングと前記第４のタイミングを比較する第２の比較手段と、
前記第２の比較手段の比較結果に基づいて、前記第１の情報処理装置との認証処理を実行する第２の認証手段とを備えることを特徴とする情報処理システム。
【請求項２８】　ネットワークを介して相互に接続される、オンオフを入力する第１の入力手段と、前記第１の入力手段によりオンが入力された第１のタイミングを計測する第1のタイミング計測手段と、前記第１の入力手段によりオフが入力された第２のタイミングを計測する第２のタイミング計測手段と、前記第２のタイミングを前記ネットワークを介して第２の情報処理装置に送信する第１の送信手段とを備えた第１の情報処理装置と、オンオフを入力する第２の入力手段と、前記第２の入力手段によりオンが入力された第３のタイミングを計測する第３のタイミング計測手段と前記第２の入力手段によりオフが入力された第４のタイミングを計測する第４のタイミング計測手段と、前記第３のタイミングを前記ネットワークを介して第１の情報処理装置に送信する第２の送信手段とを備えた前記第２の情報処理装置から構成された情報処理システムの情報処理方法において、
前記第１の情報処理装置の情報処理方法は、
前記第２の情報処理装置より送信されてくる、前記第３のタイミングを受信する第１の受信ステップと、
前記第１のタイミングと前記第３のタイミングを比較する第１の比較ステップと、
前記第１の比較ステップの処理での比較結果に基づいて、前記第２の情報処理装置との認証処理を実行する第１の認証ステップとを含み、
前記第２の情報処理装置の情報処理方法は、
前記第１の情報処理装置より送信されてくる、前記第２のタイミングを受信する第２の受信ステップと、
前記第２のタイミングと前記第４のタイミングを比較する第２の比較ステップと、
前記第２の比較ステップの処理での比較結果に基づいて、前記第１の情報処理装置との認証処理を実行する第２の認証ステップとを含むことを特徴とする情報処理システムの情報処理方法。
【請求項２９】　ネットワークを介して相互に接続される、オンオフを入力する第１の入力手段と、前記第１の入力手段によりオンが入力された第１のタイミングを計測する第1のタイミング計測手段と、前記第１の入力手段によりオフが入力された第２のタイミングを計測する第２のタイミング計測手段と、前記第２のタイミングを前記ネットワークを介して第２の情報処理装置に送信する第１の送信手段とを備えた第１の情報処理装置と、オンオフを入力する第２の入力手段と、前記第２の入力手段によりオンが入力された第３のタイミングを計測する第３のタイミング計測手段と前記第２の入力手段によりオフが入力された第４のタイミングを計測する第４のタイミング計測手段と、前記第３のタイミングを前記ネットワークを介して第１の情報処理装置に送信する第２の送信手段とを備えた第２の情報処理装置から構成された情報処理システムを制御するプログラムであって、
前記第１の情報処理装置を制御するプログラムは、
前記第２の情報処理装置より送信されてくる、前記第３のタイミングの受信を制御する第１の受信制御ステップと、
前記第１のタイミングと前記第３のタイミングとの比較を制御する第１の比較制御ステップと、
前記第１の比較制御ステップの処理での比較結果に基づいて、前記第２の情報処理装置との認証処理の実行を制御する第１の認証制御ステップとを含み、
前記第２の情報処理装置を制御するプログラムは、
前記第１の情報処理装置より送信されてくる、前記第２のタイミングの受信を制御する第２の受信制御ステップと、
前記第２のタイミングと前記第４のタイミングとの比較を制御する第２の比較制御ステップと、
前記第２の比較制御ステップの処理での比較結果に基づいて、前記第１の情報処理装置との認証処理の実行を制御する第２の認証制御ステップとを含むことを特徴とするコンピュータが読み取り可能なプログラムが記録されている記録媒体。
【請求項３０】　ネットワークを介して相互に接続される、オンオフを入力する第１の入力手段と、前記第１の入力手段によりオンが入力された第１のタイミングを計測する第1のタイミング計測手段と、前記第１の入力手段によりオフが入力された第２のタイミングを計測する第２のタイミング計測手段と、前記第２のタイミングを前記ネットワークを介して第２の情報処理装置に送信する第１の送信手段とを備えた第１の情報処理装置と、オンオフを入力する第２の入力手段と、前記第２の入力手段によりオンが入力された第３のタイミングを計測する

第３のタイミング計測手段と前記第２の入力手段によりオフが入力された第４のタイミングを計測する第４のタイミング計測手段と、前記第３のタイミングを前記ネットワークを介して第１の情報処理装置に送信する第２の送信手段とを備えた第２の情報処理装置から構成された情報処理システムを制御するコンピュータのうち、

前記第１の情報処理装置を制御するコンピュータに、

前記第２の情報処理装置より送信されてくる、前記第３のタイミングの受信を制御する第１の受信制御ステップと、

前記第１のタイミングと前記第３のタイミングとの比較を制御する第１の比較制御ステップと、

前記第１の比較制御ステップの処理での比較結果に基づいて、前記第２の情報処理装置との認証処理の実行を制御する第１の認証制御ステップとを実行させ、

前記第２の情報処理装置を制御するコンピュータに、

前記第１の情報処理装置より送信されてくる、前記第２のタイミングの受信を制御する第２の受信制御ステップと、

前記第２のタイミングと前記第４のタイミングとの比較を制御する第２の比較制御ステップと、

前記第２の比較制御ステップの処理での比較結果に基づいて、前記第１の情報処理装置との認証処理の実行を制御する第２の認証制御ステップとを実行させるプログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、情報処理装置および方法、情報処理システム、記録媒体、並びにプログラムに関し、特に、簡易に電子機器間の相互認証処理を実行できるようにした情報処理装置および方法、記録媒体、情報処理システム、並びにプログラムに関する。

【０００２】

【従来の技術】ブルートゥースを利用した至近距離での電子機器間の無線通信技術が一般に普及しつつある。

【０００３】ブルートゥースは、2.45GHzの周波数帯域を利用した無線通信技術で、到達距離は最大約10m程度のものである。類似した通信方法として赤外線通信があるが、ブルートゥースの場合は無線通信であるため障害物を通しても通信することが可能であり、その点が、赤外線通信と異なり、メリットとなっている。

【０００４】ブルートゥースにより、例えば、図１に示すように、パーソナルコンピュータ（PC：Personal Computer）１とカムコーダ２（図１（Ａ））、携帯電話機３とハンディカムコーダ４（図１（Ｂ））、カムコーダ２と携帯情報端末機５（図１（Ｃ））、および、携帯型パーソナルコンピュータ６と携帯情報通信端末機５（図１（Ｄ））などの間で、無線通信による情報の授受が可能とされる。

【０００５】このように特に配線を必要としないブルートゥースの無線接続により、例えば、携帯情報端末機５のデータを異なる部屋に存在する携帯型パーソナルコンピュータ６に転送したり、携帯電話機３をユーザの衣服のポケットに入れたままハンディカムコーダ４と接続し、ハンディカムコーダ４に記録されている映像をインターネットを介して他の電子機器に送信するということも可能である。

【０００６】これらの電子機器間での通信を行うためには、通信による誤動作、誤接続、または、データ転送時のデータの漏洩などを防止するため、それぞれの電子機器間で、１回目の通信で相互認証処理を実行させる。このとき、ユーザは必要に応じて、英数字などからなるパスワードの入力を、それぞれの電子機器で行い、認証処理を実行させる。

【０００７】ここで、例えば、図１（Ａ）で示す、パーソナルコンピュータ１とカムコーダ２の間で最初に行われる認証処理について、図２のフローチャートを参照して説明する。

【０００８】ステップＳ１において、パーソナルコンピュータ１（以下においては、PC１とも称する）は、キーボードなどの入力部より、ブルートゥースの規格上でPIN（Personal Identification Number）と呼ばれるユーザを特定するパスワードが入力されたか否かを判定し、入力されるまでその処理を繰り返し、入力されたと判定された場合、その処理は、ステップＳ２に進む。このとき、カムコーダ２も、ステップＳ２１において、同様の処理を実行する。

【０００９】ステップＳ２において、PC１は、乱数R0を発生しカムコーダ２に送信し、ステップＳ３において、乱数R0、PIN、および、BDADDR-Cam（Blue-tooth Device Address for Camcoder：カムコーダ２を識別する固有の番号）から所定の関数E22により共通鍵E22（R0,PIN,BDADDR-Cam）を演算する。ここで、BDADDR-Camは、ユーザがPC１と接続しようとする電子機器（今の場合、カムコーダ２）を指定することで選択される。

【００１０】ステップＳ２２において、カムコーダ２は、ステップＳ３の処理でPC１が使用したものと同様の関数E22により、乱数R0、PIN、および、BDADDR-Camから共通鍵CK（＝E22（R0,PIN,BDADDR-Cam））を演算し、PC１の応答として送信する。

【００１１】ステップＳ４において、PC１は、認証用の乱数R1を発生し、カムコーダ２に送信すると共に、ステップＳ５において、乱数R1、共通鍵CK、および、BDADDR-Camより、関数E1を用いてパスワードA（＝E1（R1,CK,BDADDR-Cam））を演算する。

【００１２】このとき、ステップＳ２３において、カムコーダ２は、PC１より送信されてきた乱数R1、共通鍵、および、BDADDR-Camより、ステップＳ４の処理でPC１により使用されたものと同様の関数E1によりパスワードA'（＝E1（R1,CK,BDADDR-Cam））を演算し、PC１に送信す

る。

【００１３】ステップＳ６において、ＰＣ１は、自らが演算したパスワードAと、カムコーダ２より送信されてきたパスワードA'が一致するか否かを判定し、一致したと判定した場合、ステップＳ７において、パスワードが一致したことをカムコーダ２に通知する。

【００１４】ステップＳ２４において、カムコーダ２は、ＰＣ１からの通知を受信し、ステップＳ２５において、パスワードAとパスワードA'が一致したか否かを判定する。今の場合、ステップＳ７の処理によりパスワードが一致している通知がPC１より送信されてきているので、ステップＳ２６において、認証用の乱数R2を発生し、ＰＣ１に送信すると共に、ステップＳ２７において、乱数R2、共通鍵CK、および、BDADDR-PCより、認証用の関数パスワードB（＝E1（R2,CK,BDADDR-PC））を生成する。一方、ステップＳ８において、ＰＣ１は、カムコーダ２より送信されてきた乱数R2、共通鍵CK、および、BDADDR-PCより、関数E1を使用してパスワードB'（＝E1（R2,CK,BDADDR-PC））を演算し、カムコーダ２に送信する。

【００１５】ステップＳ２８において、カムコーダ２は、パスワードＢとパスワードＢ'が一致したか否かを判定し、一致したと判定した場合、その処理は、ステップＳ２９において、認証が認められたことを認識し、同時に、パスワードＢとパスワードＢ'が一致したことをＰＣ１に送信する。ステップＳ９において、ＰＣ１は、通知を受信し、パスワードが一致し、認証が認められたことが認識する。

【００１６】ステップＳ６において、パスワードAとパスワードA'が一致しないと判定された場合、ステップＳ１０において、パスワードAとパスワードA'が一致しなかったことをカムコーダ２に通知し、その処理を終了する。

【００１７】この場合、ステップＳ２４では、パスワードAとパスワードA'が一致しなかったことを示す通知が、カムコーダ２に受信されるので、ステップＳ２５において、カムコーダ２は、パスワードAとパスワードA'が一致しなかったと判定し、その処理は、終了する。

【００１８】ステップＳ２８において、パスワードBとパスワードB'が一致しないと判定された場合、ステップＳ３０において、カムコーダ２は、認証が認められないことを認識し、パスワードBとパスワードB'が一致しなかったことを示す通知をPC１に送信する。

【００１９】そして、２回目以降の接続では、通信させようとする電子機器が、１回目の認証処理で記憶されたパスワードA,Bや、最初の接続で生成された共通鍵CKなどを利用して自動認証を行うことにより、ユーザによるパスワードの入力処理が省略されるようになっている。

【００２０】

【発明が解決しようとする課題】しかしながら、上記のような構成では、ＰＣ１とカムコーダ２や、LAN（Local Area Network）内の無線アクセスポイントに接続するなど、固定的な通信相手に対して行う場合、あまり問題とならないが、例えば、ＰＣ１上で実行させるアプリケーションソフトウェアなどにより他の電子機器と一時的に画像データなどを交換し、次のタイミングでは、通信相手を変えるような場合、新しい接続相手となる他の電子機器と接続する度に、毎回パスワードの入力が必要となるため、その処理が面倒なものであったと言う課題があった。

【００２１】本発明はこのような状況に鑑みてなされたものであり、ブルートゥースによる無線通信を実行する際、最初の相互認証を簡易な処理で実行できるようにするものである。

【００２２】

【課題を解決するための手段】本発明の第１の情報処理装置は、オンオフを入力する入力手段と、入力手段によりオンが入力された第１のタイミングを計測する第1のタイミング計測手段と、入力手段によりオフが入力された第２のタイミングを計測する第２のタイミング計測手段と、第１のタイミング、および、第２のタイミングをネットワークを介して他の情報処理装置に送信する送信手段とを備えることを特徴とする。

【００２３】前記ネットワークは、ブルートゥースにより構成されるようにすることができる。

【００２４】前記第１のタイミング計測手段、および、第２のタイミング計測手段には、いずれも複数回数のタイミングを計測させるようにすることができる。

【００２５】本発明の第１の情報処理方法は、オンオフを入力する入力手段と、入力ステップの処理でオンが入力された第１のタイミングを計測する第1のタイミング計測ステップと、入力ステップの処理でオフが入力された第２のタイミングを計測する第２のタイミング計測ステップと、第１のタイミング、および、第２のタイミングをネットワークを介して他の情報処理装置に送信する送信ステップとを含むことを特徴とする。

【００２６】第１の記録媒体のプログラムは、オンオフの入力を制御する入力制御手段と、入力制御ステップの処理でオンが入力された第１のタイミングの計測を制御する第1のタイミング計測制御ステップと、入力制御ステップの処理でオフが入力された第２のタイミングの計測を制御する第２のタイミング計測制御ステップと、第１のタイミング、および、第２のタイミングのネットワークを介した他の情報処理装置への送信を制御する送信制御ステップとを含むことを特徴とするコンピュータが読み取り可能なプログラムが記録されている。

【００２７】本発明の第１のプログラムは、オンオフの入力を制御する入力制御手段と、入力制御ステップの処理でオンが入力された第１のタイミングの計測を制御する第1のタイミング計測制御ステップと、入力制御ステップの処理でオフが入力された第２のタイミングの計測

を制御する第２のタイミング計測制御ステップと、第１のタイミング、および、第２のタイミングのネットワークを介した他の情報処理装置への送信を制御する送信制御ステップとを実行させる。

【００２８】本発明の第２の情報処理装置は、オンオフを入力する入力手段と、入力手段によりオンが入力された第１のタイミングを計測する第1のタイミング計測手段と、入力手段によりオフが入力された第２のタイミングを計測する第２のタイミング計測手段と、他の情報処理装置より送信されてくる、他の情報処理装置の他の入力手段によりオンが入力された第３のタイミング、および、オフが入力された第４のタイミングを受信する受信手段と、第１のタイミングと第３のタイミング、および、第２のタイミングと第４のタイミングを、それぞれ比較する比較手段と、比較手段の比較結果に基づいて、他の情報処理装置との認証処理を実行する認証手段とを備えることを特徴とする。

【００２９】前記ネットワークは、ブルートゥースにより構成されるようにすることができる。

【００３０】前記比較手段には、第１のタイミングと第３のタイミング、および、第２のタイミングと第４のタイミングとの、それぞれの差を求めて、差が所定範囲内であるか否かを比較させるようにすることができる。

【００３１】前記認証手段には、それぞれの差が、いずれも所定の範囲内であるとき、他の情報処理装置を認証させるようにすることができる。

【００３２】前記第１のタイミング計測手段、および、第２のタイミング計測手段には、いずれも複数回数のタイミングを計測させ、受信手段には、他の入力手段により複数回数オンが入力された第３のタイミング、および、複数回数オフにされた第４のタイミングを受信させるようにする。

【００３３】本発明の第２の情報処理方法は、オンオフを入力する入力ステップと、入力ステップの処理でオンが入力された第１のタイミングを計測する第1のタイミング計測ステップと、入力ステップの処理でオフが入力された第２のタイミングを計測する第２のタイミング計測ステップと、他の情報処理装置より送信されてくる、他の情報処理装置の他の入力ステップの処理でオンが入力された第３のタイミング、および、オフが入力された第４のタイミングを受信する受信手段と、第１のタイミングと第３のタイミング、および、第２のタイミングと第４のタイミングを、それぞれ比較する比較ステップと、比較ステップの処理での比較結果に基づいて、他の情報処理装置との認証処理を実行する認証ステップとを含むことを特徴とする。

【００３４】本発明の第２の記録媒体のプログラムは、オンオフの入力を制御する入力ステップと、入力制御ステップの処理でオンが入力された第１のタイミングの計測を制御する第1のタイミング計測制御ステップと、入力制御ステップの処理でオフが入力された第２のタイミングの計測を制御する第２のタイミング計測制御ステップと、他の情報処理装置より送信されてくる、他の情報処理装置の他の入力制御ステップの処理でオンが入力された第３のタイミング、および、オフが入力された第４のタイミングの受信を制御する受信制御手段と、第１のタイミングと第３のタイミング、および、第２のタイミングと第４のタイミングの、それぞれの比較を制御する比較制御ステップと、比較制御ステップの処理での比較結果に基づいて、他の情報処理装置との認証処理の実行を制御する認証制御ステップとを含むことを特徴とする。

【００３５】本発明の第２のプログラムは、オンオフの入力を制御する入力ステップと、入力制御ステップの処理でオンが入力された第１のタイミングの計測を制御する第1のタイミング計測制御ステップと、入力制御ステップの処理でオフが入力された第２のタイミングの計測を制御する第２のタイミング計測制御ステップと、他の情報処理装置より送信されてくる、他の情報処理装置の他の入力制御ステップの処理でオンが入力された第３のタイミング、および、オフが入力された第４のタイミングの受信を制御する受信制御手段と、第１のタイミングと第３のタイミング、および、第２のタイミングと第４のタイミングの、それぞれの比較を制御する比較制御ステップと、比較制御ステップの処理での比較結果に基づいて、他の情報処理装置との認証処理の実行を制御する認証制御ステップとを実行させる。

【００３６】本発明の第１の情報処理システムは、第1の情報処理装置が、オンオフを入力する第１の入力手段と、第１の入力手段によりオンが入力された第１のタイミングを計測する第1のタイミング計測手段と、第１の入力手段によりオフが入力された第２のタイミングを計測する第２のタイミング計測手段と、第１のタイミング、および、第２のタイミングをネットワークを介して第２の情報処理装置に送信する送信手段とを備え、第２の情報処理装置が、オンオフを入力する第２の入力手段と、第２の入力手段によりオンが入力されたタイミングを計測する第３のタイミング計測手段と、第２の入力手段によりオフが入力されたタイミングを計測する第４のタイミング計測手段と、第１の情報処理装置より送信されてくる、第１のタイミング、および、第２のタイミングを受信する受信手段と、第１のタイミングと第３のタイミング、および、第２のタイミングと第４のタイミングとをそれぞれ比較する比較手段と、比較手段の比較結果に基づいて、第１の情報処理装置との認証処理を実行する認証手段とを備えることを特徴とする。

【００３７】本発明の第１の情報処理システムの情報処理方法は、第1の情報処理装置の情報処理方法が、オンオフを入力する第１の入力ステップと、第１の入力ステップの処理でオンが入力された第１のタイミングを計測

する第1のタイミング計測ステップと、第１の入力ステップの処理でオフが入力された第２のタイミングを計測する第２のタイミング計測ステップと、第１のタイミング、および、第２のタイミングをネットワークを介して第２の情報処理装置に送信する送信ステップとを含み、第２の情報処理装置の情報処理方法は、オンオフを入力する第２の入力ステップと、第２の入力ステップの処理でオンが入力されたタイミングを計測する第３のタイミング計測ステップと、第２の入力ステップの処理でオフが入力されたタイミングを計測する第４のタイミング計測ステップと、第１の情報処理装置より送信されてくる、第１のタイミング、および、第２のタイミングを受信する受信ステップと、第１のタイミングと第３のタイミング、および、第２のタイミングと第４のタイミングとをそれぞれ比較する比較ステップと、比較ステップの処理での比較結果に基づいて、第１の情報処理装置との認証処理を実行する認証ステップとを含むことを特徴とする。

【００３８】本発明の第３の記録媒体のプログラムは、第1の情報処理装置を制御するプログラムが、オンオフの入力を制御する第１の入力制御ステップと、第１の入力制御ステップの処理でオンが入力された第１のタイミングの計測を制御する第1のタイミング計測制御ステップと、第１の入力制御ステップの処理でオフが入力された第２のタイミングの計測を制御する第２のタイミング計測制御ステップと、第１のタイミング、および、第２のタイミングのネットワークを介した第２の情報処理装置への送信を制御する送信制御ステップとを含み、第２の情報処理装置を制御するプログラムが、オンオフの入力を制御する第２の入力制御ステップと、第２の入力制御ステップの処理でオンが入力されたタイミングの計測を制御する第３のタイミング計測制御ステップと、第２の入力制御ステップの処理でオフが入力されたタイミングの計測を制御する第４のタイミング計測制御ステップと、第１の情報処理装置より送信されてくる、第１のタイミング、および、第２のタイミングの受信を制御する受信制御ステップと、第１のタイミングと第３のタイミング、および、第２のタイミングと第４のタイミングとのそれぞれの比較を制御する比較制御ステップと、比較制御ステップの処理での比較結果に基づいて、第１の情報処理装置との認証処理の実行を制御する認証制御ステップとを含むことを特徴とする。

【００３９】本発明の第３のプログラムは、第1の情報処理装置を制御するコンピュータに、オンオフの入力を制御する第１の入力制御ステップと、第１の入力制御ステップの処理でオンが入力された第１のタイミングの計測を制御する第1のタイミング計測制御ステップと、第１の入力制御ステップの処理でオフが入力された第２のタイミングの計測を制御する第２のタイミング計測制御ステップと、第１のタイミング、および、第２のタイミングのネットワークを介した第２の情報処理装置への送信を制御する送信制御ステップとを実行させ、第２の情報処理装置を制御するコンピュータに、オンオフの入力を制御する第２の入力制御ステップと、第２の入力制御ステップの処理でオンが入力されたタイミングの計測を制御する第３のタイミング計測制御ステップと、第２の入力制御ステップの処理でオフが入力されたタイミングの計測を制御する第４のタイミング計測制御ステップと、第１の情報処理装置より送信されてくる、第１のタイミング、および、第２のタイミングの受信を制御する受信制御ステップと、第１のタイミングと第３のタイミング、および、第２のタイミングと第４のタイミングとのそれぞれの比較を制御する比較制御ステップと、比較制御ステップの処理での比較結果に基づいて、第１の情報処理装置との認証処理の実行を制御する認証制御ステップとを実行させる。

【００４０】本発明の第３の情報処理装置は、オンオフを入力する入力手段と、入力手段によりオンが入力された第１のタイミングを計測する第1のタイミング計測手段と、入力手段によりオフが入力された第２のタイミングを計測する第２のタイミング計測手段と、第１のタイミング、または、第２のタイミングをネットワークを介して他の情報処理装置に送信する送信手段と、他の情報処理装置より送信されてくる、送信手段により送信された第１のタイミング、または、第２のタイミングのいずれかに対応した、他の情報処理装置の他の入力手段によりオンが入力された第３のタイミング、または、オフが入力された第４のタイミングを受信する受信手段と、第１のタイミングと第３のタイミング、または、第２のタイミングと第４のタイミングとを比較する比較手段と、比較手段の比較結果に基づいて、他の情報処理装置との認証処理を実行する認証手段とを備えることを特徴とする。

【００４１】前記ネットワークは、ブルートゥースにより構成されるようにすることができる。

【００４２】前記第１のタイミング計測手段、および、第２のタイミング計測手段には、いずれも複数回数のタイミングを計測させ、受信手段には、他の入力手段により複数回数オンが入力された第３のタイミング、および、複数回数オフにされた第４のタイミングを受信させるようにすることができる。

【００４３】前記比較手段には、第１のタイミングと第３のタイミング、または、第２のタイミングと第４のタイミングとの差を求めて、差が所定範囲内になるか否かを比較させるようにすることができる。

【００４４】前記認証手段には、差が、所定の範囲内であるとき、他の情報処理装置を認証させるようにすることができる。

【００４５】本発明の第３の情報処理方法は、オンオフを入力する入力ステップと、入力ステップの処理でオン

が入力された第１のタイミングを計測する第1のタイミング計測ステップと、入力ステップの処理でオフが入力された第２のタイミングを計測する第２のタイミング計測ステップと、第１のタイミング、または、第２のタイミングをネットワークを介して他の情報処理装置に送信する送信ステップと、他の情報処理装置より送信されてくる、送信ステップの処理で送信された第１のタイミング、または、第２のタイミングのいずれかに対応した、他の情報処理装置の他の入力ステップの処理でオンが入力された第３のタイミング、または、オフが入力された第４のタイミングを受信する受信ステップと、第１のタイミングと第３のタイミング、または、第２のタイミングと第４のタイミングとを比較する比較ステップと、比較ステップの処理での比較結果に基づいて、他の情報処理装置との認証処理を実行する認証ステップとを含むことを特徴とする。

【００４６】本発明の第４の記録媒体のプログラムは、オンオフの入力を制御する入力制御ステップと、入力制御ステップの処理でオンが入力された第１のタイミングの計測を制御する第1のタイミング計測制御ステップと、入力制御ステップの処理でオフが入力された第２のタイミングの計測を制御する第２のタイミング計測制御ステップと、第１のタイミング、または、第２のタイミングのネットワークを介した他の情報処理装置への送信を制御する送信制御ステップと、他の情報処理装置より送信されてくる、送信制御ステップの処理で送信された第１のタイミング、または、第２のタイミングのいずれかに対応した、他の情報処理装置の他の入力制御ステップの処理でオンが入力された第３のタイミング、または、オフが入力された第４のタイミングの受信を制御する受信制御ステップと、第１のタイミングと第３のタイミング、または、第２のタイミングと第４のタイミングとの比較を制御する比較制御ステップと、比較制御ステップの処理での比較結果に基づいて、他の情報処理装置との認証処理の実行を制御する認証制御ステップとを含むことを特徴とする。

【００４７】本発明の第４のプログラムは、オンオフの入力を制御する入力制御ステップと、入力制御ステップの処理でオンが入力された第１のタイミングの計測を制御する第1のタイミング計測制御ステップと、入力制御ステップの処理でオフが入力された第２のタイミングの計測を制御する第２のタイミング計測制御ステップと、第１のタイミング、または、第２のタイミングのネットワークを介した他の情報処理装置への送信を制御する送信制御ステップと、他の情報処理装置より送信されてくる、送信制御ステップの処理で送信された第１のタイミング、または、第２のタイミングのいずれかに対応した、他の情報処理装置の他の入力制御ステップの処理でオンが入力された第３のタイミング、または、オフが入力された第４のタイミングの受信を制御する受信制御ステップと、第１のタイミングと第３のタイミング、または、第２のタイミングと第４のタイミングとの比較を制御する比較制御ステップと、比較制御ステップの処理での比較結果に基づいて、他の情報処理装置との認証処理の実行を制御する認証制御ステップとを実行させる。

【００４８】本発明の第２の情報処理システムは、第１の情報処理装置が、第２の情報処理装置より送信されてくる、第３のタイミングを受信する第１の受信手段と、第１のタイミングと第３のタイミングを比較する第１の比較手段と、第１の比較手段の比較結果に基づいて、第２の情報処理装置との認証処理を実行する第１の認証手段とを備え、第２の情報処理装置が、第１の情報処理装置より送信されてくる、第２のタイミングを受信する第２の受信手段と、第２のタイミングと第４のタイミングを比較する第２の比較手段と、第２の比較手段の比較結果に基づいて、第１の情報処理装置との認証処理を実行する第２の認証手段とを備えることを特徴とする。

【００４９】本発明の第２の情報処理システムの情報処理方法は、第１の情報処理装置の情報処理方法が、第２の情報処理装置より送信されてくる、第３のタイミングを受信する第１の受信ステップと、第１のタイミングと第３のタイミングを比較する第１の比較ステップと、第１の比較ステップの処理での比較結果に基づいて、第２の情報処理装置との認証処理を実行する第１の認証ステップとを含み、第２の情報処理装置の情報処理方法が、第１の情報処理装置より送信されてくる、第２のタイミングを受信する第２の受信ステップと、第２のタイミングと第４のタイミングを比較する第２の比較ステップと、第２の比較ステップの処理での比較結果に基づいて、第１の情報処理装置との認証処理を実行する第２の認証ステップとを含むことを特徴とする。

【００５０】本発明の第５の記録媒体のプログラムは、第１の情報処理装置を制御するプログラムが、第２の情報処理装置より送信されてくる、第３のタイミングの受信を制御する第１の受信制御ステップと、第１のタイミングと第３のタイミングとの比較を制御する第１の比較制御ステップと、第１の比較制御ステップの処理での比較結果に基づいて、第２の情報処理装置との認証処理の実行を制御する第１の認証制御ステップとを含み、第２の情報処理装置を制御するプログラムが、第１の情報処理装置より送信されてくる、第２のタイミングの受信を制御する第２の受信制御ステップと、第２のタイミングと第４のタイミングとの比較を制御する第２の比較制御ステップと、第２の比較制御ステップの処理での比較結果に基づいて、第１の情報処理装置との認証処理の実行を制御する第２の認証制御ステップとを含むことを特徴とする。

【００５１】本発明の第５のプログラムは、第１の情報処理装置を制御するコンピュータに、第２の情報処理装置より送信されてくる、第３のタイミングの受信を制御

する第１の受信制御ステップと、第１のタイミングと第３のタイミングとの比較を制御する第１の比較制御ステップと、第１の比較制御ステップの処理での比較結果に基づいて、第２の情報処理装置との認証処理の実行を制御する第１の認証制御ステップとを実行させ、第２の情報処理装置を制御するコンピュータに、第１の情報処理装置より送信されてくる、第２のタイミングの受信を制御する第２の受信制御ステップと、第２のタイミングと第４のタイミングとの比較を制御する第２の比較制御ステップと、第２の比較制御ステップの処理での比較結果に基づいて、第１の情報処理装置との認証処理の実行を制御する第２の認証制御ステップとを実行させる。

【００５２】本発明の第１の情報処理装置および方法、並びにプログラムにおいては、オンオフが入力され、オンが入力された第１のタイミングが計測され、オフが入力された第２のタイミングが計測され、第１のタイミング、および、第２のタイミングがネットワークを介して他の情報処理装置に送信される。

【００５３】本発明の第２の情報処理装置および方法、並びにプログラムにおいては、オンオフが入力され、オンが入力された第１のタイミングが計測され、オフが入力された第２のタイミングが計測され、他の情報処理装置より送信されてくる、他の情報処理装置にオンが入力された第３のタイミング、および、オフが入力された第４のタイミングが受信され、第１のタイミングと第３のタイミング、および、第２のタイミングと第４のタイミングが、それぞれ比較され、比較結果に基づいて、他の情報処理装置との認証処理が実行される。

【００５４】本発明の第１の情報処理システムおよび方法、並びにプログラムにおいては、第1の情報処理装置により、オンオフが入力され、オンが入力された第１のタイミングが計測され、オフが入力された第２のタイミングが計測され、第１のタイミング、および、第２のタイミングがネットワークを介して第２の情報処理装置に送信され、第２の情報処理装置により、オンオフが入力され、オンが入力されたタイミングが計測され、オフが入力されたタイミングが計測され、第１の情報処理装置より送信されてくる、第１のタイミング、および、第２のタイミングが受信され、第１のタイミングと第３のタイミング、および、第２のタイミングと第４のタイミングとがそれぞれ比較され、比較結果に基づいて、第１の情報処理装置との認証処理が実行される。

【００５５】本発明の第３の情報処理装置および方法、並びにプログラムにおいては、オンオフが入力され、オンが入力された第１のタイミングが計測され、オフが入力された第２のタイミングが計測され、第１のタイミング、または、第２のタイミングがネットワークを介して他の情報処理装置に送信され、他の情報処理装置より送信されてくる、送信された第１のタイミング、または、第２のタイミングのいずれかに対応した、他の情報処理装置のオンが入力された第３のタイミング、または、オフが入力された第４のタイミングが受信され、第１のタイミングと第３のタイミング、または、第２のタイミングと第４のタイミングとが比較され、比較結果に基づいて、他の情報処理装置との認証処理が実行される。

【００５６】本発明の第２の情報処理システムおよび方法、並びにプログラムにおいては、第１の情報処理装置により、第２の情報処理装置より送信されてくる、第３のタイミングが受信され、第１のタイミングと第３のタイミングが比較され、比較結果に基づいて、第２の情報処理装置との認証処理が実行され、第２の情報処理装置により、第１の情報処理装置より送信されてくる、第２のタイミングが受信され、第２のタイミングと第４のタイミングが比較され、比較結果に基づいて、第１の情報処理装置との認証処理が実行される。

【００５７】

【発明の実施の形態】図３は、本発明に係る無線通信システムの一実施の形態の構成を示す図である。尚、図３以降の図面の説明においては、従来の場合と対応する部分には同一の符号を付してあり、その説明は適宜省略する。パーソナルコンピュータ１とカムコーダ２は、上述のブルートゥースを用いることにより相互にデータを無線通信で交換することができる。

【００５８】図４は、本発明を適用したパーソナルコンピュータ１とカムコーダ２の構成を示したブロック図である。まず、パーソナルコンピュータ１の構成について説明する。パーソナルコンピュータ１のマイクロコンピュータ２１は、CPU（CentralProcessing Unit）、ROM（Read Only Memory）、および、RAM（Random AccessMemory）から構成されており、CPUが、ROMに記憶されたプログラムを適宜RAMに読込んで、各種の処理を実行する。また、マイクロコンピュータ２１は、パーソナルコンピュータ１の全体の動作を制御しており、バス２７を介してハードディスク２２に記憶されている、認証プログラム２２ａを始めとした各種のプログラムを内部のRAMに展開させて、各種の処理を実行する。さらに、マイクロコンピュータ２１は、バス２７を介してドライブ２０１に装着された磁気ディスク２１１、光ディスク２１２、光磁気ディスク２１３、または、半導体メモリ２１４に記憶された各種のプログラムを読込んで実行すると共に、必要に応じて、各種のプログラムやデータを書き込む。

【００５９】ハードディスク２２は、通信部２５により接続されるカムコーダ２などの電子機器間の認証処理を実行する認証プログラム２２ａを始めとして、各種のプログラムを記憶すると共に、プログラムの実行に必要なデータを記憶する。表示部２３は、マイクロコンピュータ２１により制御され、CRT（Cathode Ray Tube）やLCD（Liquid Crystal Display）などからなり、各種の処理結果や、後述する操作用のウィンドウを表示する。認証

プログラム22aは、認証ボタン26の押下されたタイミング、押下が終了したタイミングのそれぞれの時刻を計測し、これをカムコーダ2より送信されてくる、同様のタイミングの時刻とを、カムコーダ2の基準時刻と自らの基準時刻との時間差を考慮して比較し、比較結果に基づいて認証処理を実行する。PC1の自らの基準時刻は、図示せぬリアルタイムクロックより発生されている。

【0060】入力部24は、キーボードやマウスなどからなりユーザが、各種のコマンドを入力するとき操作される。通信部25は、いわゆるブルートゥースにより構成されており、マイクロコンピュータ21からの指令に基づいて、無線によりカムコーダ2を始めとした電子機器と各種データの授受を実行する。認証ボタン26は、認証しようとするカムコーダ2と、ブルートゥースにより規定された最初の認証処理を行うとき、認証しようとするカムコーダ2に設けられた認証ボタン35と同時に操作され、同じタイミングでオンオフされることにより、認証処理を実行させるためのものである。認証ボタン26，35の操作の詳細については後述する。

【0061】次に、カムコーダ2の構成について説明する。カムコーダ2のマイクロコンピュータ31は、カムコーダ2の全体の動作を制御しており、CPU、ROM、および、RAMから構成されている。マイクロコンピュータ31のCPUは、ROMに記憶された各種のプログラムを適宜RAMに読込んで各種の処理を実行する。また、マイクロコンピュータ31は、バス41に接続されたハードディスク32に記憶された、認証プログラム32aを始めとして、各種のプログラムを読込んで実行する。認証プログラム32aは、認証ボタン35の押下されたタイミング、押下が終了したタイミングのそれぞれの時刻を計測し、これらをPC1より送信されてくる、同様のタイミングを示す時刻と、PC1の基準時刻と自らの基準時刻との時間差を考慮して比較し、比較結果に基づいて認証処理を実行する。カムコーダ2の自らの基準時刻は、図示せぬリアルタイムクロックより発生されている。

【0062】表示部33は、撮像部34により撮像された画像や、メカデッキ39に装着された記録媒体に記録された画像を表示させる。撮像部34は、CCD（Charge Coupled Device）カメラなどからなり、図示せぬ被写体を撮像して画像データを生成する。通信部36は、上述と同様のブルートゥースから構成されており、マイクロコンピュータ31により制御され、無線通信によりPC1と各種のデータを授受する。

【0063】入力部37は、タブレットボタンなどから構成されており、ユーザが、各種のコマンドを入力するとき操作される。記録再生制御部38は、マイクロコンピュータ31からの指令に基づいて、撮像部34により撮像された画像・音声データを所定の方式で圧縮して、メカデッキ39に装着された記録媒体に記録すると共に、記録媒体に記録された圧縮された画像・音声データを伸長し、元の画像・音声データとして再生して、表示部33に表示する。

【0064】次に、PC1の認証ボタン26と、カムコーダ2の認証ボタン35の認証操作について説明する。認証を行う際、ユーザは、認証させようとするPC1とカムコーダ2のそれぞれに設けられた認証ボタン26，35を、同じタイミングで押下する。双方の認証プログラム22a，32aは、相互の認証ボタン26，35が押下された時刻と、押下が終了された時刻をそれぞれ相互に測定し、無線通信により相互に授受し、同じタイミングで押下されたことが認識されると、認証が成立するというものである。すなわち、相互認証しようとする電子機器同士でなければ、認証ボタン26，35が同じタイミングで押下される可能性は、極めて低く、逆に、相互の認証ボタン26，35が同じタイミングで操作されれば、相互に認証処理がなされているものであるとみなし、認証を成立させるというものである。

【0065】ただし、ユーザによる操作であるため（人間により操作されるものであるので）、それぞれの認証ボタン26，35を同時に押下したつもりでも、厳密に同じタイミングで押下することはできないことがある。そこで、タイミングには、余裕が持たせてある。

【0066】すなわち、図5（A）に示すように、PC1の認証ボタン26が押下されたタイミングをタイミングｔA1とし、認証ボタン26の押下が終了したタイミングをタイミングｔA2であるとし、さらに、カムコーダ2の認証ボタン35の押下されたタイミングをタイミングｔB1とし、押下が終了したタイミングをタイミングｔB2とする。この場合、例えば、カムコーダ2の認証ボタン35が押下されたタイミングを基準とすると、前後に時間ｅ（＝200ms程度）の余裕を持たせて、タイミングｔA1が、ｔB1－ｅ＜ｔA1＜ｔB1＋ｅを満たし、かつ、時刻ｔA2が、ｔB2－ｅ＜ｔA2＜ｔB2＋ｅを満たすとき、双方の認証ボタン26，35は、同時に押下されたものとみなす。これにより、押下されたタイミング（時刻）が、ユーザの（人間の）操作により生じてしまう程度の誤差範囲内で同時に押下されれば、相互の電子機器は認証を成立させることができる。尚、以上の説明においては、カムコーダ2の認証ボタン35が押下されたタイミングを基準として説明してきたが、当然のことながら、PC1の認証ボタン26が押下されたタイミングを基準としても同様である。また、上述の例では、PC1、および、カムコーダ2の相互に認証用の専用ボタンである認証ボタン26，35をそれぞれに操作した場合について説明してきたが、必ずしも専用のボタンを設ける必要はなく、例えば、PC1については、キーボードの所定のボタンを押下することで代用させるようにしてもよいし、カムコーダ2については、停止ボタンなどの認証処理時に動作に寄与しないボタンな

どで代用させるようにしても良い。認証ボタン２６，３５は、押下できるもの、或いは、オンオフを切替えられるものであれば、必ずしもボタンでなくても良く、例えば、ジョグダイヤルに代表される、回転押圧式操作素子などにより認証ボタン２６，３５を代用させるようにしても良いし、タッチパネルなどにより、ユーザに触れられているか否かによりオンオフが切替えられるものであればよい。

【００６７】次に、図６のフローチャートを参照して、PC１とカムコーダ２が認証処理を実行するときの動作について説明する。

【００６８】ステップＳ４１において、PC１の認証プログラム２２ａは、認証ボタン２６がオンにされたか（押下されたか）否かを判定し、オンにされたと判定されるまで同様の処理を繰り返し、認証ボタン２６がオンにされたと判定された場合、ステップＳ４２において、認証プログラム２２ａは、認証ボタン２６がオンにされた、すなわち、押下されたタイミングである時刻ｔＡ１を測定し記憶する。

【００６９】ステップＳ４３において、PC１の認証プログラム２２ａは、認証ボタン２６がオフにされたか（押下された状態が解除されたか）否かを判定し、オフにされたと判定されるまで同様の処理を繰り返し、認証ボタン２６がオフにされたと判定された場合、ステップＳ４４において、認証プログラム２２ａは、認証ボタン２６がオフにされた、すなわち、押下された状態が解除されたタイミングである時刻ｔＡ２を測定し記憶する。

【００７０】このとき、ステップＳ６１乃至Ｓ６４において、カムコーダ２の認証プログラム３２ａもPC１の認証プログラム２２ａと同様の処理を実行する。すなわち、ステップＳ６１において、カムコーダ２の認証プログラム３２ａは、認証ボタン３５がオンにされたか（押下されたか）否かを判定し、オンにされたと判定されるまで同様の処理を繰り返し、認証ボタン３５がオンにされたと判定された場合、ステップＳ６２において、認証プログラム３２ａは、認証ボタン３５がオンにされた、すなわち、押下されたタイミングである時刻ｔＢ１を測定し記憶する。

【００７１】ステップＳ６３において、カムコーダ２の認証プログラム３２ａは、認証ボタン３５がオフにされたか（押下された状態が解除されたか）否かを判定し、オフにされたと判定されるまで同様の処理を繰り返し、認証ボタン３５がオフにされたと判定された場合、ステップＳ６４において、認証プログラム３２ａは、認証ボタン３５がオフにされた、すなわち、押下された状態が解除されたタイミングである時刻ｔＢ２を測定し記憶する。

【００７２】ステップＳ４５において、PC１の認証プログラム２２ａは、通信部２５を制御して、基準時刻ｔＡ０をカムコーダ２に送信する。

【００７３】ステップＳ６５において、カムコーダ２の認証プログラム３２ａは、通信部３６を制御して、基準タイミングｔＡ０を受信したか否かを判定し、基準時刻ｔＡ０が受信されるまで、その処理を繰り返し、受信したと判定された場合、ステップＳ６６において、自らの基準時刻との時間差（ｔＢ０－ｔＡ０）を演算し、時刻ｔＢ１，ｔＢ２を補正する。すなわち、PC１で計測されたタイミングとカムコーダ２で計測されたタイミングを比較することになるので、PC１の基準時刻、すなわち、例えば、基準時刻を送信する際のPC１のリアルタイムクロックで計測された時刻ｔＡ０を送信すると、カムコーダ２は、これを受信し、自らの基準時刻ｔＢ０との差を求めて、PC１との時間差を求め、これを利用して、以下の式（１），式（２）に示すように、自らが計測した時刻ｔＢ１，ｔＢ２から、その時間差を減算して求める。

$$t_{B1}(\text{補正後}) = t_{B1}(\text{補正前}) - (t_{B0} - t_{A0}) \cdots (1)$$

$$t_{B2}(\text{補正後}) = t_{B2}(\text{補正前}) - (t_{B0} - t_{A0}) \cdots (2)$$

【００７４】ステップＳ４６において、認証プログラム２２ａは、通信部２５を制御して、時刻ｔＡ１，ｔＡ２をカムコーダ２に送信する。

【００７５】ステップＳ６７において、カムコーダ２の認証プログラム３２ａは、PC１より時刻ｔＡ１，ｔＡ２の情報を受信したか否かを判定し、受信するまでその処理を繰り返し、受信したと判定した場合、その処理は、ステップＳ６８に進む。

【００７６】ステップＳ６８において、認証プログラム３２ａは、ｔＡ１がｔＢ１－ｅ＜ｔＡ１＜ｔＢ１＋ｅを満たしているか否かを判定し、例えば、図５に示すように、満たしていると判定された場合、その処理は、ステップＳ６９に進む。

【００７７】ステップＳ６９において、認証プログラム３２ａは、ｔＡ２がｔＢ２－ｅ＜ｔＡ２＜ｔＢ２＋ｅを満たしているか否かを判定し、例えば、図５に示すように、満たしていると判定された場合、ステップＳ７０において、認証が認められたことをPC１に通知する。

【００７８】ステップＳ４７において、PC１の認証プログラム２２ａは、通知を受信したか否かを判定し、通知が受信されるまで同様の処理を繰り返し、例えば、ステップＳ７０の処理により、認証が認められた通知が受信されると、ステップＳ４８において、PC１の認証プログラム２２ａは、認証結果を認識し、今の場合、認証が認められたことを認識する。

【００７９】ステップＳ６８，Ｓ６９において、ｔＡ１がｔＢ１－ｅ＜ｔＡ１＜ｔＢ１＋ｅを満たしていない、または、ｔＡ２がｔＢ２－ｅ＜ｔＡ２＜ｔＢ２＋ｅを満たしていないと判定された場合、ステップＳ７１において、認証プログラム３２ａは、認証が認められなかっ

た、すなわち、認証ボタン２６，３５が同時に操作されなかったとみなし、通信部３６を制御して、認証が認められなかったことをPC１に通知する。

【００８０】以上の例においては、カムコーダ２側でPC１とカムコーダ２の認証ボタン２６，３５が同時に操作されたかを認証判定する処理について説明してきたが、当然のことながら、PC１側で認証判定処理（図６のステップＳ６８，６９の処理）を実行するようにしてもよい。

【００８１】また、認証判定処理は、PC１とカムコーダ２で、相互に実行するようにしてもよく、その場合の処理について、図７のフローチャートを参照して説明する。

【００８２】ステップＳ８１において、PC１の認証プログラム２２ａは、認証ボタン２６がオンにされたか（押下されたか）否かを判定し、オンにされたと判定されるまで同様の処理を繰り返し、認証ボタン２６がオンにされたと判定された場合、ステップＳ８２において、認証プログラム２２ａは、認証ボタン２６がオンにされた、すなわち、押下されたタイミングである時刻ｔＡ１を測定し記憶する。

【００８３】ステップＳ８３において、PC１の認証プログラム２２ａは、認証ボタン２６がオフにされたか（押下された状態が解除されたか）否かを判定し、オフにされたと判定されるまで同様の処理を繰り返し、認証ボタン２６がオフにされたと判定された場合、ステップＳ８４において、認証プログラム２２ａは、認証ボタン２６がオフにされた、すなわち、押下された状態が解除されたタイミングである時刻ｔＡ２を測定し記憶する。

【００８４】このとき、ステップＳ１０１乃至Ｓ１０４において、カムコーダ２の認証プログラム３２ａもPC１の認証プログラム２２ａと同様の処理を実行する。すなわち、ステップＳ１０１において、カムコーダ２の認証プログラム３２ａは、認証ボタン３５がオンにされたか（押下されたか）否かを判定し、オンにされたと判定されるまで同様の処理を繰り返し、認証ボタン３５がオンにされたと判定された場合、ステップＳ１０２において、認証プログラム３２ａは、認証ボタン３５がオンにされた、すなわち、押下されたタイミングである時刻ｔＢ１を測定し記憶する。

【００８５】ステップＳ１０３において、カムコーダ２の認証プログラム３２ａは、認証ボタン３５がオフにされたか（押下された状態が解除されたか）否かを判定し、オフにされたと判定されるまで同様の処理を繰り返し、認証ボタン３５がオフにされたと判定された場合、ステップＳ１０４において、認証プログラム３２ａは、認証ボタン３５がオフにされた、すなわち、押下された状態が解除されたタイミングである時刻ｔＢ２を測定し記憶する。

【００８６】ステップＳ８５において、PC１の認証プログラム２２ａは、通信部２５を制御して、基準時刻ｔＡ０をカムコーダ２に送信する。

【００８７】ステップＳ１０５において、カムコーダ２の認証プログラム３２ａは、通信部３６を制御して、基準タイミングｔＡ０を受信したか否かを判定し、基準時刻ｔＡ０が受信されるまで、その処理を繰り返し、受信したと判定された場合、ステップＳ１０６において、自らの基準時刻との時間差（ｔＢ０－ｔＡ０）を演算し、時刻ｔＢ１，ｔＢ２を補正する。

【００８８】ステップＳ８６において、認証プログラム２２ａは、通信部２５を制御して、時刻ｔＡ１，ｔＡ２をカムコーダ２に送信する。

【００８９】ステップＳ１０７において、カムコーダ２の認証プログラム３２ａは、PC１より時刻ｔＡ１，ｔＡ２の情報を受信したか否かを判定し、受信するまでその処理を繰り返し、受信したと判定した場合、その処理は、ステップＳ１０８に進む。

【００９０】ステップＳ１０８において、認証プログラム３２ａは、ｔＡ１がｔＢ１－ｅ＜ｔＡ１＜ｔＢ１＋ｅを満たしているか否かを判定し、例えば、図８（Ｂ）に示すように、満たしていると判定された場合、その処理は、ステップＳ１０９に進む。

【００９１】ステップＳ１０９において、認証プログラム３２ａは、通信部３６を制御して、認証が認められたことをPC１に通知する。

【００９２】ステップＳ８７において、PC１の認証プログラム２２ａは、通知を受信したか否かを判定し、通知が受信されるまで同様の処理を繰り返し、例えば、ステップＳ１０９の処理により、認証が認められた通知が受信されると、その処理は、ステップＳ８８に進む。

【００９３】ステップＳ１１０において、認証プログラム３２ａは、通信部３６を制御して、時刻ｔＢ２をPC１に送信する。

【００９４】ステップＳ８８において、PC１の認証プログラム２２ａは、通信部２５を制御して、時刻ｔＢ２をカムコーダ２より受信したか否かを判定し、受信されるまで、その処理を繰り返し、受信されたと判定された場合、その処理は、ステップＳ８９に進む。

【００９５】ステップＳ８９において、認証プログラム２２ａは、ｔＢ２がｔＡ２－ｅ＜ｔＢ２＜ｔＡ２＋ｅを満たしているか否かを判定し、例えば、図８（Ａ）に示すように、満たしていると判定された場合、ステップＳ９０において、通信部２５を制御して、認証が認められたことをカムコーダ２に通知する。

【００９６】ステップＳ１１１において、カムコーダ２の認証プログラム３２ａは、PC１から送信されてくる認証結果を受信し、認識する。例えば、ステップＳ９０の処理により送信されてくる認証結果により認証が認められたことを認識する。

【００９７】ステップＳ１０８において、ｔＡ１がｔＢ

１－ｅ＜ｔＡ１＜ｔＢ１＋ｅを満たしていないと判定された場合、ステップＳ１１２において、認証プログラム３２ａは、認証が認められなかった、すなわち、認証ボタン２６，３５が同時に操作されなかったとみなし、通信部３６を制御して、認証が認められなかったことをPC１に通知する。

【００９８】結果として、ステップＳ８７において、認証プログラム２２ａは、認証が認められなかったと判定し、その処理は終了する。

【００９９】また、ステップＳ８９において、ｔＢ２がｔＡ２－ｅ＜ｔＢ２＜ｔＡ２＋ｅを満たしていないと判定された場合、ステップＳ９１において、PC１の認証プログラム２２ａは、通信部２５を制御して認証が認められなかったことをカムコーダ２に送信する。

【０１００】以上のように、カムコーダ２では、認証ボタン２６，３５が押下されたタイミングの時刻が比較され、PC１では、認証ボタン２６，３５の押下が解除されたタイミングの時刻が比較されることにより、相互で認証処理を行うことができる。もちろん、以上の例とは、逆に、PC１が、認証ボタン２６，３５が押下されたタイミングの時刻を比較し、カムコーダ２が、認証ボタン２６，３５の押下が解除されたタイミングの時刻を比較するようにしてもよい。

【０１０１】また、以上の例においては、認証ボタン２６，３５が相互に１回だけ押下された場合の処理について説明してきたが、１回の押下では、誤操作などにより偶然に認証が認められてしまう可能性がある。このため、認証ボタン２６，３５を押下する回数は、複数回数にするようにして、誤操作の発生を防止させることもできる。

【０１０２】そこで、次に、認証ボタン２６，３５を相互に複数回数ずつ押下する場合（例えば、ｎ回押下する場合）について、図９のフローチャートを参照して説明する。このとき、認証プログラム２２ａ，３２ａは、押下された回数をカウントするためのカウンタｉをそれぞれ備える。

【０１０３】ステップＳ１２１において、PC１の認証プログラム２２ａは、自らのカウンタｉを１に初期化する。ステップＳ１２２において、PC１の認証プログラム２２ａは、認証ボタン２６がオンにされたか（押下されたか）否かを判定し、オンにされたと判定されるまで同様の処理を繰り返し、認証ボタン２６がオンにされたと判定された場合、ステップＳ１２３において、認証プログラム２２ａは、認証ボタン２６がオンにされた、すなわち、押下されたタイミングである時刻ｔＡｉを測定し記憶する。

【０１０４】ステップＳ１２４において、PC１の認証プログラム２２ａは、認証ボタン２６がオフにされたか（押下された状態が解除されたか）否かを判定し、オフにされたと判定されるまで同様の処理を繰り返し、認証ボタン２６がオフにされたと判定された場合、ステップＳ１２５において、認証プログラム２２ａは、認証ボタン２６がオフにされた、すなわち、押下された状態が解除されたタイミングである時刻ｔＡ（ｉ＋１）を測定し記憶する。ステップＳ１２６において、認証プログラム２２ａは、カウンタｉを２だけインクリメントする。ステップＳ１２７において、カウンタｉ／２がｎより大きいか否かを判定し、カウンタｉ／２がｎより大きくないと判定された場合、その処理は、ステップＳ１２２に戻りそれ以降の処理が繰り返され、認証ボタン２６が押下されるべき設定回数であるｎよりもｉ／２が大きくなるまで、ステップＳ１２２乃至Ｓ１２６の処理が繰り返される。ステップＳ１２７において、カウンタｉ／２が認証ボタン２６が押下される所定回数ｎより大きいと判定された場合、その処理は、ステップＳ１２８に進む。

【０１０５】このとき、ステップＳ１４１乃至Ｓ１４７において、カムコーダ２の認証プログラム３２ａもPC１の認証プログラム２２ａと同様の処理を実行する。すなわち、ステップＳ１４１において、カムコーダ２の認証プログラム３２ａは、自らのカウンタｉを１に初期化する。ステップＳ１４２において、カムコーダ２の認証プログラム３２ａは、認証ボタン３５がオンにされたか（押下されたか）否かを判定し、オンにされたと判定されるまで同様の処理を繰り返し、認証ボタン３５がオンにされたと判定された場合、ステップＳ１４３において、認証プログラム３２ａは、認証ボタン３５がオンにされた、すなわち、押下されたタイミングである時刻ｔＢｉを測定し記憶する。

【０１０６】ステップＳ１４４において、カムコーダ２の認証プログラム３２ａは、認証ボタン３５がオフにされたか（押下された状態が解除されたか）否かを判定し、オフにされたと判定されるまで同様の処理を繰り返し、認証ボタン３５がオフにされたと判定された場合、ステップＳ１４５において、認証プログラム３２ａは、認証ボタン３５がオフにされた、すなわち、押下された状態が解除されたタイミングである時刻ｔＢ（ｉ＋１）を測定し記憶する。

【０１０７】ステップＳ１４６において、カムコーダ２の認証プログラム３２ａは、カウンタｉを２だけインクリメントする。ステップＳ１４７において、カウンタｉ／２がｎより大きいか否かを判定し、カウンタｉ／２がｎより大きくないと判定された場合、その処理は、ステップＳ１４２に戻りそれ以降の処理が繰り返され、認証ボタン２６が押下されるべき設定回数であるｎよりもｉ／２が大きくなるまで、ステップＳ１４２乃至Ｓ１４６の処理が繰り返される。ステップＳ１４７において、カウンタｉ／２が認証ボタン３５が押下される所定回数ｎより大きいと判定された場合、その処理は、ステップＳ１４８に進む。

【０１０８】ステップＳ１２８において、PC１の認証プ

ログラム22aは、通信部25を制御して、基準時刻tA0をカムコーダ2に送信する。

【0109】ステップS148において、カムコーダ2の認証プログラム32aは、通信部36を制御して、基準タイミングtA0を受信したか否かを判定し、基準時刻tA0が受信されるまで、その処理を繰り返し、受信したと判定された場合、ステップS149において、自らの基準時刻との時間差(tB0-tA0)を演算し、時刻tB1，tB2・・・，tB(2n)を補正する。

【0110】ステップS129において、認証プログラム22aは、通信部25を制御して、時刻tA1，tA2・・・，tA(2n)をカムコーダ2に送信する。

【0111】ステップS150において、カムコーダ2の認証プログラム32aは、PC1より時刻tA1，tA2・・・，tA(2n)の情報を受信したか否かを判定し、受信するまでその処理を繰り返し、受信したと判定した場合、その処理は、ステップS151に進む。

【0112】ステップS151において、認証プログラム32aは、全てのi(i=1乃至2n)について、tAiがtBi-e<tAi<tBi+eを満たしているか否かを判定し、例えば、図10に示すように、tB1-e<tA1<tB1+e，tB2-e<tA2<tB2+e，tB3-e<tA3<tB3+e，tB4-e<tA4<tB4+e，・・・tB(2n-1)-e<tA(2n-1)<tB(2n-1)+e、tB(2n)-e<tA(2n)<tB(2n)+e満たしていると判定された場合、その処理は、ステップS152に進む。ステップS152において、認証プログラム32aは、認証が認められたことをPC1に通知する。

【0113】ステップS130において、PC1の認証プログラム22aは、通知を受信したか否かを判定し、通知が受信されるまで同様の処理を繰り返し、例えば、ステップS152の処理により、認証が認められた通知が受信されると、ステップS131において、PC1の認証プログラム22aは、認証結果を認識し、今の場合、認証が認められたことを認識する。

【0114】ステップS151において、全てのi(i=1乃至2n)について、tAiがtBi-e<tAi<tBi+eを満たしていないと判定された場合、ステップS153において、認証プログラム32aは、認証が認められなかった、すなわち、認証ボタン26，35が同時に操作されなかったとみなし、通信部36を制御して、認証が認められなかったことをPC1に通知する。

【0115】以上の例においては、カムコーダ2側でPC1とカムコーダ2の認証ボタン26，35が、複数回数に渡って同時に操作されたかを認証判定する処理について説明してきたが、当然のことながら、PC1側で認証判定処理(図9のステップS151の処理)を実行するようにしてもよい。

【0116】また、認証ボタン26，35を複数回数押下する場合でも、図7のフローチャートを参照して説明したように、認証判定処理は、PC1とカムコーダ2で、相互に実行するようにしてもよく、その場合の処理について、図11のフローチャートを参照して説明する。

【0117】ステップS171において、PC1の認証プログラム22aは、自らのカウンタiを1に初期化する。ステップS172において、PC1の認証プログラム22aは、認証ボタン26がオンにされたか(押下されたか)否かを判定し、オンにされたと判定されるまで同様の処理を繰り返し、認証ボタン26がオンにされたと判定された場合、ステップS173において、認証プログラム22aは、認証ボタン26がオンにされた、すなわち、押下されたタイミングである時刻tAiを測定し記憶する。

【0118】ステップS174において、PC1の認証プログラム22aは、認証ボタン26がオフにされたか(押下された状態が解除されたか)否かを判定し、オフにされたと判定されるまで同様の処理を繰り返し、認証ボタン26がオフにされたと判定された場合、ステップS175において、認証プログラム22aは、認証ボタン26がオフにされた、すなわち、押下された状態が解除されたタイミングである時刻tA(i+1)を測定し記憶する。

【0119】ステップS176において、認証プログラム22aは、カウンタiを2だけインクリメントする。ステップS177において、カウンタi/2がnより大きいか否かを判定し、カウンタi/2がnより大きくないと判定された場合、その処理は、ステップS172に戻りそれ以降の処理が繰り返され、認証ボタン26が押下されるべき設定回数であるnよりもi/2が大きくなるまで、ステップS172乃至S176の処理が繰り返される。ステップS177において、カウンタi/2が認証ボタン26が押下される所定回数nより大きいと判定された場合、その処理は、ステップS178に進む。

【0120】このとき、ステップS201乃至S207において、カムコーダ2の認証プログラム32aもPC1の認証プログラム22aと同様の処理を実行する。すなわち、ステップS201において、カムコーダ32aは、カウンタiを1に初期化する。さらに、ステップS202において、カムコーダ2の認証プログラム32aは、認証ボタン35がオンにされたか(押下されたか)否かを判定し、オンにされたと判定されるまで同様の処理を繰り返し、認証ボタン35がオンにされたと判定された場合、ステップS203において、認証プログラム32aは、認証ボタン35がオンにされた、すなわち、押下されたタイミングである時刻tBiを測定し記憶する。

【0121】ステップS204において、カムコーダ2の認証プログラム32aは、認証ボタン35がオフにされたか(押下された状態が解除されたか)否かを判定

し、オフにされたと判定されるまで同様の処理を繰り返し、認証ボタン35がオフにされたと判定された場合、ステップS205において、認証プログラム32aは、認証ボタン35がオフにされた、すなわち、押下された状態が解除されたタイミングである時刻tB(i+1)を測定し記憶する。

【0122】ステップS206において、認証プログラム32aは、カウンタiを2だけインクリメントする。ステップS207において、カウンタi/2がnより大きいか否かを判定し、カウンタi/2がnより大きくないと判定された場合、その処理は、ステップS202に戻りそれ以降の処理が繰り返され、認証ボタン35が押下されるべき設定回数であるnよりもi/2が大きくなるまで、ステップS202乃至S206の処理が繰り返される。ステップS207において、カウンタi/2が認証ボタン35が押下される所定回数nより大きいと判定された場合、その処理は、ステップS208に進む。

【0123】ステップS178において、PC1の認証プログラム22aは、通信部25を制御して、基準時刻tA0をカムコーダ2に送信する。

【0124】ステップS208において、カムコーダ2の認証プログラム32aは、通信部36を制御して、基準タイミングtA0を受信したか否かを判定し、基準時刻tA0が受信されるまで、その処理を繰り返し、受信したと判定された場合、ステップS209において、自らの基準時刻との時間差(tB0-tA0)を演算し、時刻tB1，tB2・・・，tB(2n)を補正する。

【0125】ステップS179において、認証プログラム22aは、通信部25を制御して、tAiのうちカウンタiが奇数となる時刻tA1，tA3・・・，tA(2n-1)をカムコーダ2に送信する。

【0126】ステップS210において、カムコーダ2の認証プログラム32aは、PC1よりtAiのうちカウンタiが奇数となる時刻tA1，tA3・・・，tA(2n-1)の情報を受信したか否かを判定し、受信するまでその処理を繰り返し、受信したと判定した場合、その処理は、ステップS211に進む。

【0127】ステップS211において、認証プログラム32aは、全ての奇数のカウンタi(i=1，3，5・・・2n-1)のtAiについて、tBi-e<tAi<tBi+eを満たしているか否かを判定し、例えば、図12(B)に示すように、tB1-e<tA1<tB1+e，tB3-e<tA3<tB3+e，・・・tB(2n-1)-e<tA(2n-1)<tB(2n-1)+eを満たしていると判定された場合、その処理は、ステップS212において、認証が認められたことをPC1に通知する。

【0128】ステップS180において、PC1の認証プログラム22aは、通知を受信したか否かを判定し、通知が受信されるまで同様の処理を繰り返し、例えば、ステップS212の処理により、認証が認められた通知が受信されると、ステップS181に進む。

【0129】ステップS213において、認証プログラム32aは、通信部36を制御して、時刻tBiのうち、iが偶数の時刻tB2，tB4・・・，tB(2n)をPC1に送信する。

【0130】ステップS181において、PC1の認証プログラム22aは、通信部25を制御して、時刻tB2，tB4・・・，tB(2n)をカムコーダ2より受信したか否かを判定し、受信されるまで、その処理を繰り返し、受信されたと判定された場合、その処理は、ステップS182に進む。

【0131】ステップS182において、認証プログラム22aは、時刻tB2，tB4・・・，tB(2n)がtA2-e<tB2<tA2+e，tA4-e<tB4<tA4+e・・・tA(2n)-e<tB(2n)<tA(2n)+eを満たしているか否かを判定し、例えば、図12(A)に示すように、満たしていると判定された場合、ステップS183において、通信部25を制御して、認証が認められたことをカムコーダ2に通知する。

【0132】ステップS214において、カムコーダ2の認証プログラム32aは、PC1から送信されてくる認証結果を受信し、認識する。例えば、ステップS183の処理により送信されてくる認証結果により認証が認められたことを認識する。

【0133】ステップS211において、tAiのうちiが奇数のものがtBi-e<tAi<tBi+eを満たしていないと判定された場合、ステップS215において、認証プログラム32aは、認証が認められなかった、すなわち、認証ボタン26，35が複数回数に渡って同時に操作されなかったとみなし、通信部36を制御して、認証が認められなかったことをPC1に通知する。

【0134】結果として、ステップS180において、認証プログラム22aは、認証が認められなかったと判定し、その処理は終了する。

【0135】また、ステップS182において、tBiのうちiが偶数のものがtAi-e<tBi<tAi+eを満たしていないと判定された場合、ステップS184において、PC1の認証プログラム22aは、通信部25を制御して認証が認められなかったことをカムコーダ2に送信する。

【0136】以上のように、複数回数に渡り、PC1とカムコーダ2の相互で認証処理を実行させることもでき、認証処理時の誤動作などにも対応することができる。

【0137】以上の例においては、PC1とカムコーダ2の間での認証処理について説明してきたが、それ以外の電子機器間でも、ブルートゥースを備えた電子機器間であればよく、例えば、図1(B)乃至(D)に示すように、ブルートゥースを備えた携帯電話機3とハンディカ

ムコーダ４、カムコーダ２と携帯情報端末機５、携帯型パーソナルコンピュータ６と携帯情報端末機５などに代表される様々な電子機器間でも、同様の処理による認証処理を実現させることができる。

【０１３８】また、ブルートゥースの規格においては、PIN=0とすることによりPINの入力を省略させた状態で接続することができるようになっている。このPINの省略機能を利用して、最初の認証処理は、ブルートゥースの規格通りの認証処理として、それ以降の認証処理は、上述のように認証ボタンを用いる方法とするようにしてもよい。

【０１３９】さらに、認証処理を実行する毎に、認証ボタン２６，３５の押下回数ｎを変化させるようにしてもよい。

【０１４０】また、上述の例では、PC１とカムコーダ２の認証プログラム２２ａ，３２ａで、相互に認証処理を実行する場合、一方の認証プログラムが認証ボタン２６，３５が押下された時刻を比較し、他方の認証プログラムが認証ボタン２６，３５の押下状態が解除された時刻を比較することにより認証処理を行う例について説明してきたが、相互の認証プログラムが比較する時刻は、互いに重なり合わない時刻同士であれば、２つの集合に分けて、相互に比較するようにしてもよい。

【０１４１】さらに、相互の基準時刻ｔＡ０，ｔＢ０を使用せずに、例えば、それぞれの最初に認証ボタン２６，３５が押下されるタイミングである時刻ｔＡ１，ｔＢ１を基準として、各時刻との差を求めて、ｔＡｉ－ｔＡ１とｔＢｉ－ｔＢ１を、ｉ＝１乃至２ｎの範囲で求めて、それぞれ対応する時刻を比較するようにしてもよい。このとき、時刻ｔＡ１，ｔＢ１は、基準時刻と同様に扱われるため、タイミングを比較する時刻の数が１個分減ることになるので、１回の押下（ｎ＝１）だけでは、認証ボタン２６，３５のタイミングの差を求めることができないので、複数回数の押下の開始と終了のタイミングの時刻情報が必要となる。

【０１４２】また、本発明は、通信部２５，３６としてブルートゥースを用いた例について説明してきたが、ブルートゥース以外の通信部からなる無線通信システム、または、有線通信システム上での認証処理に使用するようにしてもよい。

【０１４３】以上によれば、簡単な操作で、認証処理を実現させることができる。

【０１４４】上述した一連の処理は、ハードウェアにより実行させることもできるが、ソフトウェアにより実行させることもできる。一連の処理をソフトウェアにより実行させる場合には、そのソフトウェアを構成するプログラムが、専用のハードウェアに組み込まれているコンピュータ、または、各種のプログラムをインストールすることで、各種の機能を実行させることが可能な、例えば汎用のパーソナルコンピュータなどに記録媒体からインストールされる。

【０１４５】この記録媒体は、図４に示すようにパーソナルコンピュータ１に予め組み込まれた状態でユーザに提供される、プログラムが記録されているハードディスク２２だけではなく、コンピュータとは別に、ユーザにプログラムを提供するために配布される、プログラムが記録されている磁気ディスク２１１（フレキシブルディスクを含む）、光ディスク２１２（CD-ROM(Compact Disc-Read Only Memory)，DVD（Digital Versatile Disc）を含む）、光磁気ディスク２１３（MD（Mini-Disc）（登録商標）を含む）、もしくは半導体メモリ２１４（Memory Stickを含む）などよりなるパッケージメディアにより構成される。

【０１４６】尚、本明細書において、記録媒体に記録されるプログラムを記述するステップは、記載された順序に沿って時系列的に行われる処理は、もちろん、必ずしも時系列的に処理されなくとも、並列的あるいは個別に実行される処理を含むものである。

【０１４７】また、本明細書において、システムとは、複数の装置により構成される装置全体を表すものである。

【０１４８】

【発明の効果】本発明の第１の情報処理装置および方法、並びにプログラムによれば、オンオフを入力し、オンを入力した第１のタイミングを計測し、オフを入力した第２のタイミングを計測し、第１のタイミング、および、第２のタイミングをネットワークを介して他の情報処理装置に送信するようにした。

【０１４９】本発明の第２の情報処理装置および方法、並びにプログラムによれば、オンオフを入力し、オンを入力した第１のタイミングを計測し、オフを入力した第２のタイミングを計測し、他の情報処理装置より送信されてくる、他の情報処理装置にオンを入力した第３のタイミング、および、オフを入力した第４のタイミングを受信し、第１のタイミングと第３のタイミング、および、第２のタイミングと第４のタイミングを、それぞれ比較し、比較結果に基づいて、他の情報処理装置との認証処理を実行するようにした。

【０１５０】本発明の第１の情報処理システムおよび方法、並びにプログラムによれば、第1の情報処理装置が、オンオフを入力し、オンを入力した第１のタイミングを計測し、オフを入力した第２のタイミングを計測し、第１のタイミング、および、第２のタイミングをネットワークを介して第２の情報処理装置に送信し、第２の情報処理装置が、オンオフを入力し、オンを入力したタイミングを計測し、オフを入力したタイミングを計測し、第１の情報処理装置より送信されてくる、第１のタイミング、および、第２のタイミングを受信し、第１のタイミングと第３のタイミング、および、第２のタイミングと第４のタイミングとをそれぞれ比較し、比較結果

に基づいて、第１の情報処理装置との認証処理を実行するようにした。

【０１５１】本発明の第３の情報処理装置および方法、並びにプログラムによれば、オンオフを入力し、オンを入力した第１のタイミングを計測し、オフを入力した第２のタイミングを計測し、第１のタイミング、または、第２のタイミングをネットワークを介して他の情報処理装置に送信し、他の情報処理装置より送信されてくる、送信された第１のタイミング、または、第２のタイミングのいずれかに対応した、他の情報処理装置にオンを入力した第３のタイミング、または、オフを入力した第４のタイミングを受信し、第１のタイミングと第３のタイミング、または、第２のタイミングと第４のタイミングとを比較し、比較結果に基づいて、他の情報処理装置との認証処理を実行するようにした。

【０１５２】本発明の第２の情報処理システムおよび方法、並びにプログラムによれば、第１の情報処理装置が、第２の情報処理装置より送信されてくる、第３のタイミングを受信し、第１のタイミングと第３のタイミングを比較し、比較結果に基づいて、第２の情報処理装置との認証処理を実行し、第２の情報処理装置が、第１の情報処理装置より送信されてくる、第２のタイミングを受信し、第２のタイミングと第４のタイミングを比較し、比較結果に基づいて、第１の情報処理装置との認証処理を実行するようにした。

【０１５３】いずれにおいても、結果として、相互認証処理を簡単に実行することが可能となる。

【図面の簡単な説明】

【図１】従来の無線接続による電子機器の組合せを示す図である。

【図２】従来の認証処理を説明するフローチャートである。

【図３】本発明を適用した無線通信システムの一実施の形態の構成を示す図である。

【図４】図３のパーソナルコンピュータとカムコーダの構成を示すブロック図である。

【図５】認証ボタンの押下のタイミングを示すタイミングチャートである。

【図６】本発明を適用した認証処理を説明するフローチャートである。

【図７】本発明を適用した認証処理を説明するフローチャートである。

【図８】認証ボタンの押下のタイミングを示すタイミングチャートである。

【図９】本発明を適用した認証処理を説明するフローチャートである。

【図１０】認証ボタンの押下のタイミングを示すタイミングチャートである。

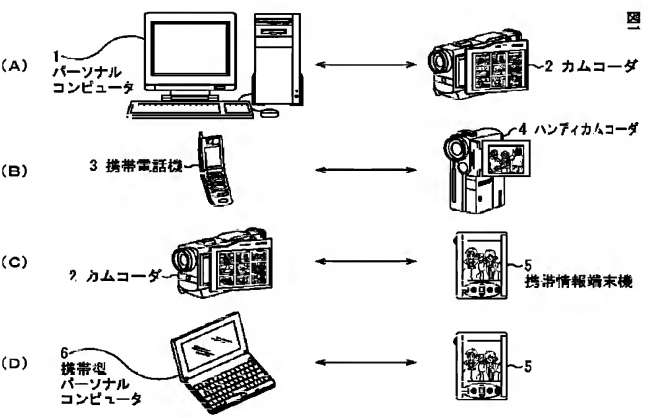
【図１１】本発明を適用した認証処理を説明するフローチャートである。

【図１２】認証ボタンの押下のタイミングを示すタイミングチャートである。

【符号の説明】

１　パーソナルコンピュータ，２　カムコーダ，２２ａ　認証プログラム，２６　認証ボタン，３２ａ　認証プログラム，３５　認証ボタン

【図１】



【図2】

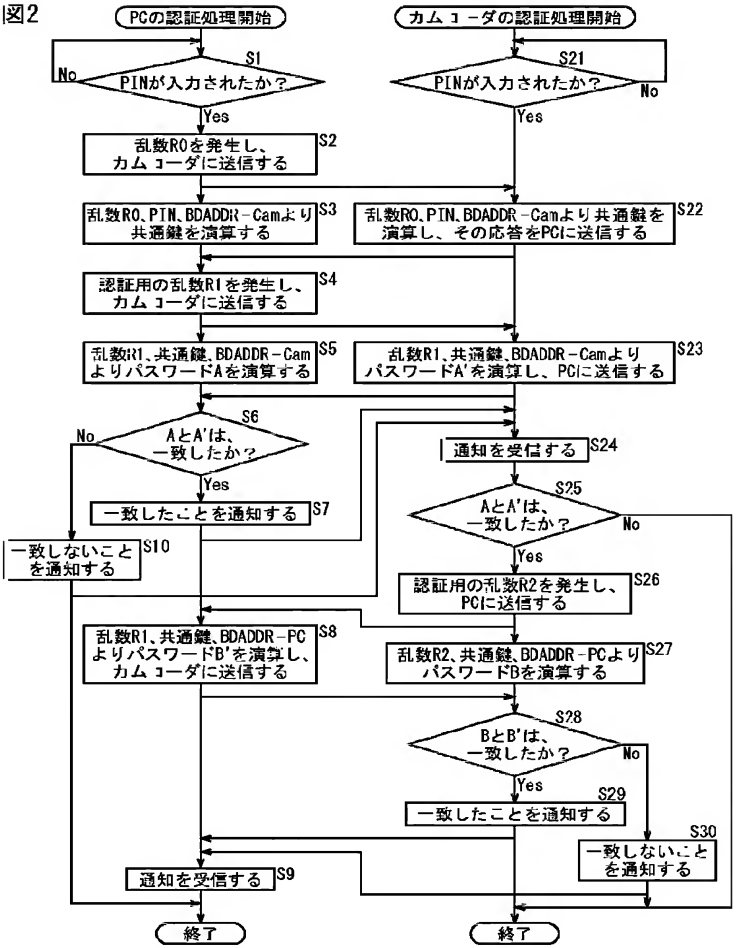
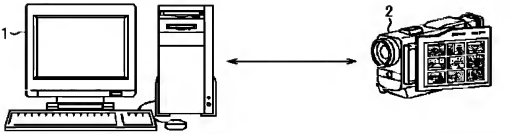


図2
PCの認証処理開始
カムコーダの認証処理開始
S1
PINが入力されたか？
No
Yes
S21
PINが入力されたか？
No
Yes
乱数R0を発生し、カムコーダに送信する
S2
乱数R0、PIN、BDADDR-Camより共通鍵を演算する
S3
乱数R0、PIN、BDADDR-Camより共通鍵を演算し、その応答をPCに送信する
S22
認証用の乱数R1を発生し、カムコーダに送信する
S4
乱数R1、共通鍵、BDADDR-CamよりパスワードAを演算する
S5
乱数R1、共通鍵、BDADDR-CamよりパスワードA'を演算し、PCに送信する
S23
S6
AとA'は、一致したか？
No
Yes
通知を受信する
S24
一致したことを通知する
S7
S25
AとA'は、一致したか？
No
Yes
一致しないことを通知する
S10
認証用の乱数R2を発生し、PCに送信する
S26
乱数R1、共通鍵、BDADDR-PCよりパスワードB'を演算し、カムコーダに送信する
S8
乱数R2、共通鍵、BDADDR-PCよりパスワードBを演算する
S27
S28
BとB'は、一致したか？
No
Yes
一致したことを通知する
S29
一致しないことを通知する
S30
通知を受信する
S9
終了
終了

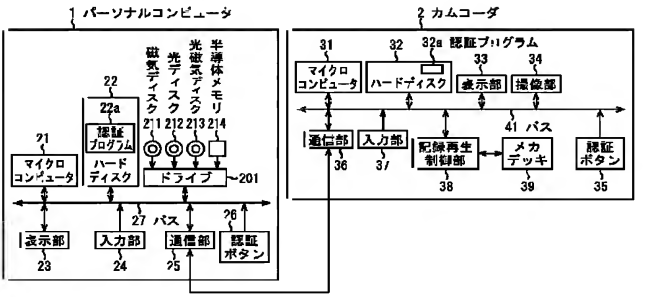
【図3】

図3



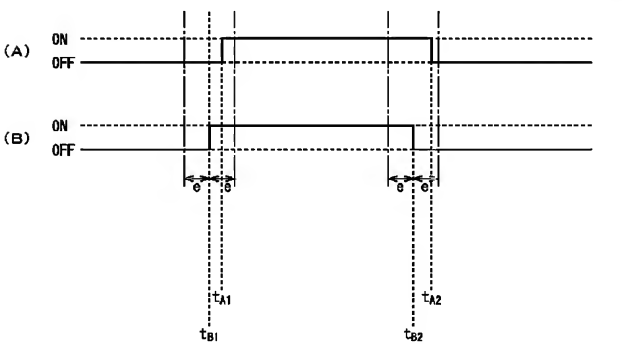
【図4】

図4



【図5】

図5



【図6】

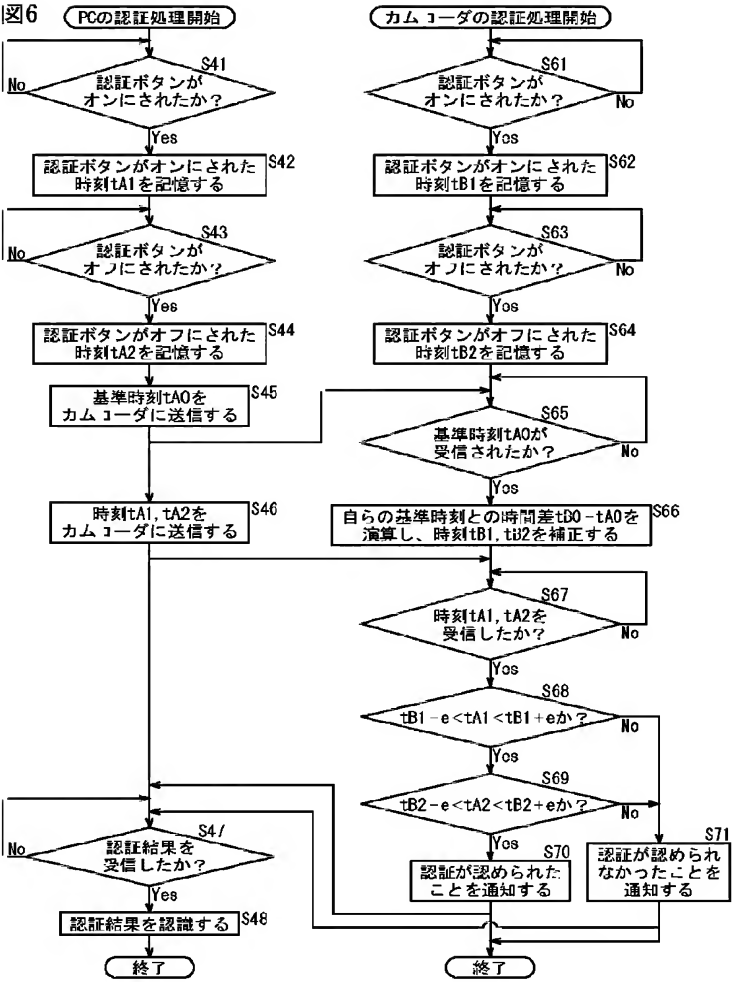
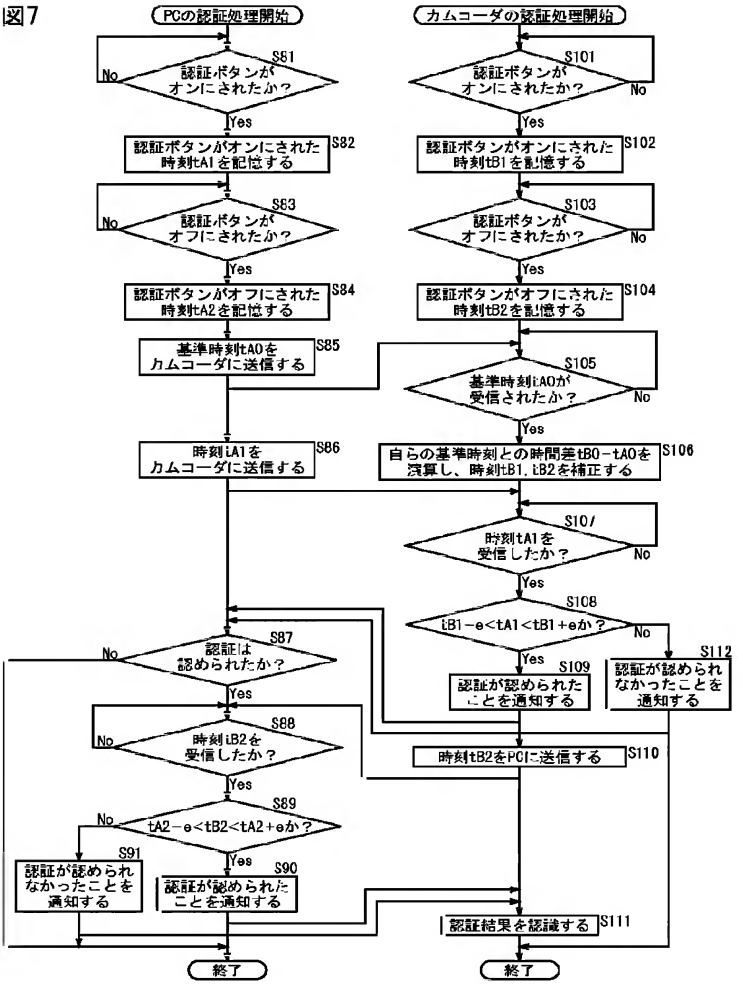


図6
PCの認証処理開始
S41
認証ボタンがオンにされたか？
No
Yes
認証ボタンがオンにされた時刻tA1を記憶する
S42
S43
認証ボタンがオフにされたか？
No
Yes
認証ボタンがオフにされた時刻tA2を記憶する
S44
基準時刻tA0をカムコーダに送信する
S45
時刻tA1, tA2をカムコーダに送信する
S46
S47
認証結果を受信したか？
No
Yes
認証結果を認識する
S48
終了
カムコーダの認証処理開始
S61
認証ボタンがオンにされたか？
No
Yes
認証ボタンがオンにされた時刻tB1を記憶する
S62
S63
認証ボタンがオフにされたか？
No
Yes
認証ボタンがオフにされた時刻tB2を記憶する
S64
S65
基準時刻tA0が受信されたか？
No
Yes
自らの基準時刻との時間差tD0−tA0を演算し、時刻tB1, tB2を補正する
S66
S67
時刻tA1, tA2を受信したか？
No
Yes
S68
tB1−e<tA1<tB1+eか？
No
Yes
S69
tB2−e<tA2<tB2+eか？
No
Yes
S70
認証が認められたことを通知する
S71
認証が認められなかったことを通知する
終了

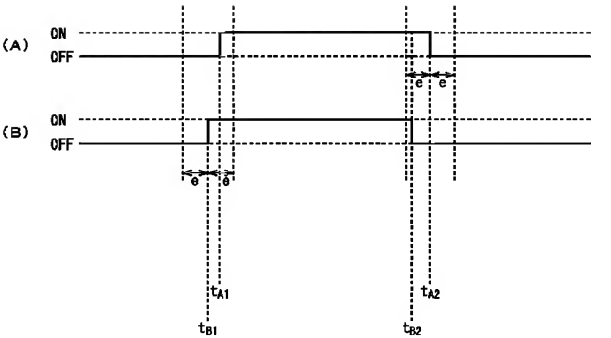
【図7】

図7


PCの認証処理開始
カムコーダの認証処理開始
S81
認証ボタンがオンにされたか？
No
Yes
S101
認証ボタンがオンにされたか？
No
Yes
S82
認証ボタンがオンにされた時刻tA1を記憶する
S102
認証ボタンがオンにされた時刻tB1を記憶する
S83
認証ボタンがオフにされたか？
No
Yes
S103
認証ボタンがオフにされたか？
No
Yes
S84
認証ボタンがオフにされた時刻tA2を記憶する
S104
認証ボタンがオフにされた時刻tB2を記憶する
S85
基準時刻tA0をカムコーダに送信する
S105
基準時刻tA0が受信されたか？
No
Yes
S86
時刻tA1をカムコーダに送信する
S106
自らの基準時刻との時間差tB0−tA0を演算し、時刻tB1,tB2を補正する
S107
時刻tA1を受信したか？
No
Yes
S108
tB1−e<tA1<tB1+eか？
No
Yes
S87
認証は認められたか？
No
Yes
S109
認証が認められたことを通知する
S112
認証が認められなかったことを通知する
S88
時刻tB2を受信したか？
No
Yes
S110
時刻tB2をPCに送信する
S89
tA2−e<tB2<tA2+eか？
No
Yes
S91
認証が認められなかったことを通知する
S90
認証が認められたことを通知する
S111
認証結果を認識する
終了
終了

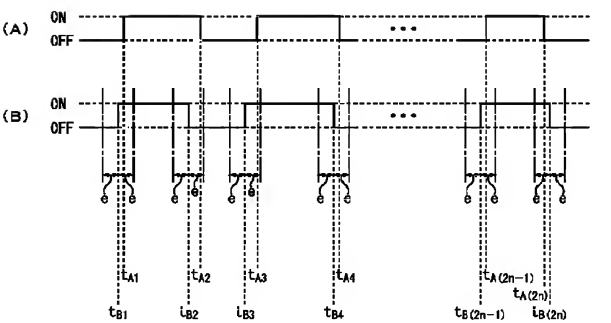
【図8】

図8


(A)
ON
OFF
(B)
ON
OFF
e
e
e
e
tA1
tB1
tA2
tB2

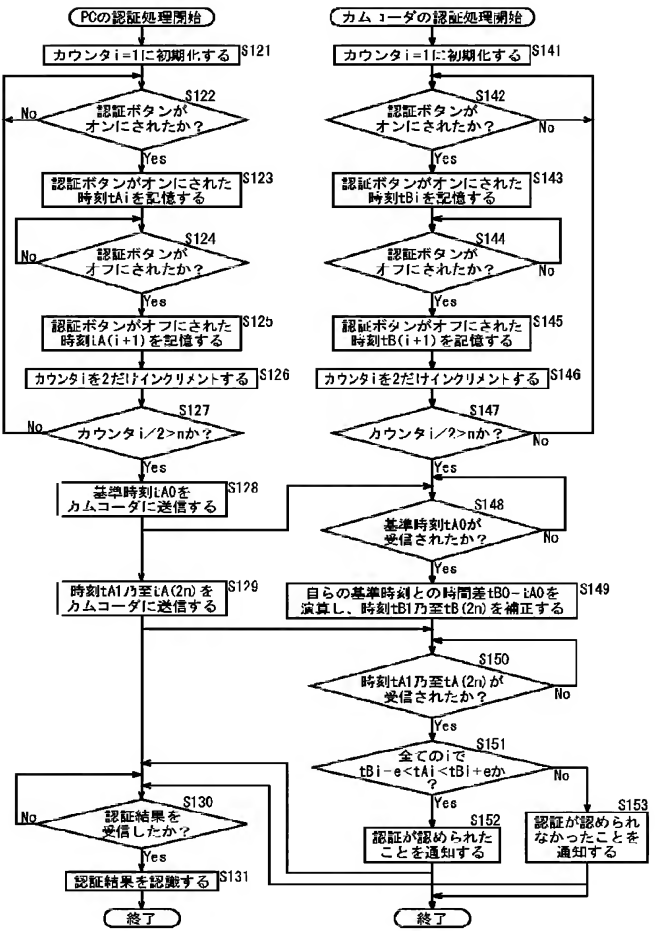
【図10】

図10


(A)
ON
OFF
(B)
ON
OFF
e
tA1
tB1
tA2
tB2
tA3
tB3
tA4
tB4
tA(2n-1)
tB(2n-1)
tA(2n)
tB(2n)

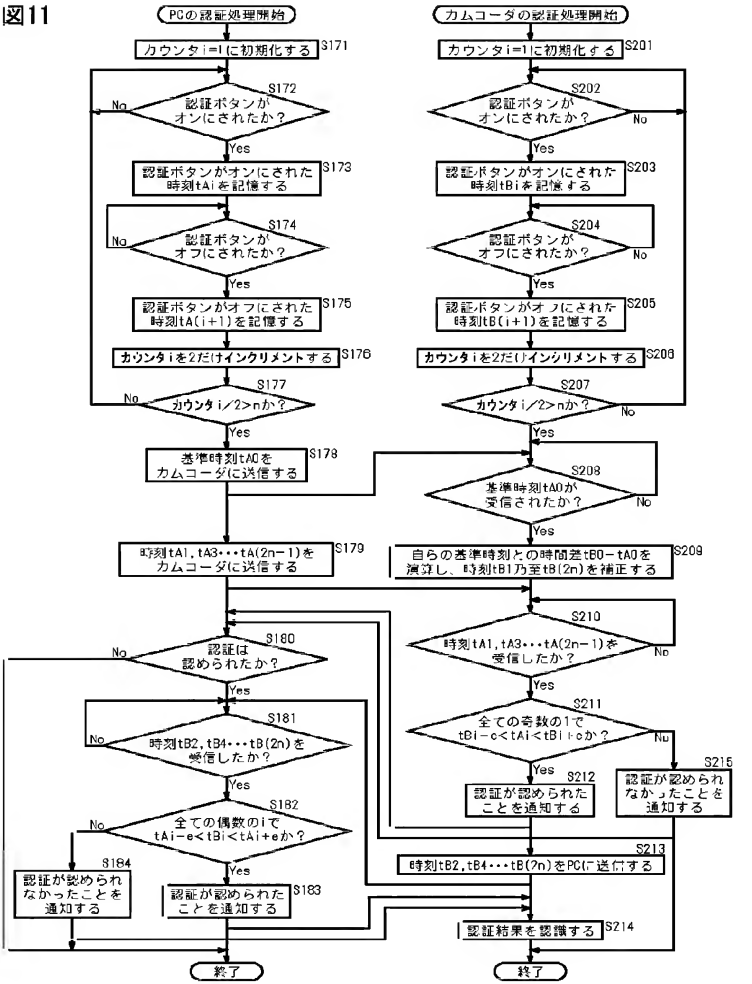
【図9】

図9


PCの認証処理開始
カムコーダの認証処理開始
カウンタi=1に初期化する S121
カウンタi=1に初期化する S141
S122
認証ボタンがオンにされたか？
No
Yes
S142
認証ボタンがオンにされたか？
No
Yes
認証ボタンがオンにされた時刻tAiを記憶する S123
認証ボタンがオンにされた時刻tBiを記憶する S143
S124
認証ボタンがオフにされたか？
No
Yes
S144
認証ボタンがオフにされたか？
No
Yes
認証ボタンがオフにされた時刻tA(i+1)を記憶する S125
認証ボタンがオフにされた時刻tB(i+1)を記憶する S145
カウンタiを2だけインクリメントする S126
カウンタiを2だけインクリメントする S146
S127
カウンタi/2>nか？
No
Yes
S147
カウンタi/2>nか？
No
Yes
基準時刻tA0をカムコーダに送信する S128
S148
基準時刻tA0が受信されたか？
No
Yes
時刻tA1乃至tA(2n)をカムコーダに送信する S129
自らの基準時刻との時間差tB0−tA0を演算し、時刻tB1乃至tB(2n)を補正する S149
S150
時刻tA1乃至tA(2n)が受信されたか？
No
Yes
S151
全てのiでtBi−e<tAi<tBi+eか？
No
Yes
S130
認証結果を受信したか？
No
Yes
S152
認証が認められたことを通知する
S153
認証が認められなかったことを通知する
認証結果を認識する S131
終了
終了

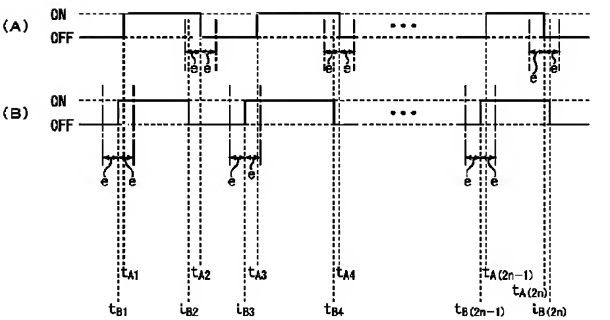
【図１１】

図11


PCの認証処理開始
カウンタi=1に初期化する
S171
認証ボタンがオンにされたか？
S172
No
Yes
認証ボタンがオンにされた時刻tAiを記憶する
S173
認証ボタンがオフにされたか？
S174
No
Yes
認証ボタンがオフにされた時刻tA(i+1)を記憶する
S175
カウンタiを2だけインクリメントする
S176
カウンタi／2>nか？
S177
No
Yes
基準時刻tA0をカムコーダに送信する
S178
時刻tA1,tA3・・・tA(2n−1)をカムコーダに送信する
S179
認証は認められたか？
S180
No
Yes
時刻tB2,tB4・・・tB(2n)を受信したか？
S181
No
Yes
全ての偶数のiでtAi−e<tBi<tAi+eか？
S182
No
Yes
認証が認められたことを通知する
S183
認証が認められなかったことを通知する
S184
終了
カムコーダの認証処理開始
カウンタi=1に初期化する
S201
認証ボタンがオンにされたか？
S202
No
Yes
認証ボタンがオンにされた時刻tBiを記憶する
S203
認証ボタンがオフにされたか？
S204
No
Yes
認証ボタンがオフにされた時刻tB(i+1)を記憶する
S205
カウンタiを2だけインクリメントする
S206
カウンタi／2>nか？
S207
No
Yes
基準時刻tA0が受信されたか？
S208
No
Yes
自らの基準時刻との時間差tB0−tA0を演算し、時刻tB1乃至tB(2n)を補正する
S209
時刻tA1,tA3・・・tA(2n−1)を受信したか？
S210
No
Yes
全ての奇数のiでtBi−c<tAi<tBi+cか？
S211
No
Yes
認証が認められたことを通知する
S212
認証が認められなかったことを通知する
S215
時刻tB2,tB4・・・tB(2n)をPCに送信する
S213
認証結果を認識する
S214
終了

【図12】

図12


(A)
ON
OFF
(B)
ON
OFF
e
tA1
tA2
tA3
tA4
tA(2n-1)
tA(2n)
tB1
tB2
tB3
tB4
tB(2n-1)
tB(2n)